RADIOFREQUENZ-IDENTIFIKATION

Interessengemeinschaft **work@it**

GPA djp
GEWERKSCHAFT DER PRIVATANGESTELLTEN
DRUCK – JOURNALISMUS – PAPIER

Impressum:

HeraugeberIn: GPA-djp, Interessengemeinschaft work@IT
Verantwortlich für den Inhalt: Arbeitsgruppe RFID, Nicholas Hauser
Layout: GPA-djp Marketing, Ulrike Pesendorfer
Fotos: GPA-djp, fotolia.com
DVR: 0046655, ÖGB ZVR-Nr.: 576439352
Dezember 2008

Mit freundlicher Unterstützung von:

ver.di-innotec gGmbH
www.verdi-innotec.de

FIfF - Forum InformatikerInnen für Frieden
und gesellschaftliche Verantwortung e.V
www.fiff.de

Vorwort

Für wenig Menschen, die wenig mit Technik vertraut sind klingt das wie Science Fiction: Winzige Chips, die Unmengen von Daten speichern können und es so ermöglichen jede Bewegung einer Ware oder auch eines Menschen zu überwachen. Seit vielen Jahren im Einzelhandel an den Kassen eingesetzt und zuletzt bei den Reispässen zur Speicherung biometrischer Daten eingeführt, spielen diese High-Tech-Spielzeuge auch am Arbeitsplatz eine immer größere Rolle.

Nicht nur Waren, sondern auch Personen lassen sich mit aktiven RFID-Tags lokalisieren. Die neue Technologie ermöglicht nicht nur Rationalisierungen, sie sind vielmehr auch ein umfassendes Dokumentations-, Registrier-, Verarbeitungs- und Auswertungs- sowie Kontroll-Werkzeug. Zusätzlich ermöglichen sie als zentraler technischer Bestandteil die überbetriebliche Vernetzung von Daten über Produkte und ihre Qualitäten genauso wie über die Arbeitnehmer/-innen und ihr Leistungsvermögen.

Da die RFID-Systeme berührungslos arbeiten, kann auf die gespeicherten Daten zugegriffen werden, ohne dass dies den betroffenen Person bewusst ist. So erhielt etwa ein Mitarbeiter eines Supermarkts einen Drohbrief von seinem Arbeitgeber, weil per Überwachungssystem festgestellt worden war, dass er an einem Tag neunmal die Toilette aufgesucht hatte. Die dort verbrachte Zeit werde ihm nun vom Gehalt abgezogen.

Für BetriebsrätInnen bedeutet das, dass sie wachsam sein müssen. Denn jeder Chip im Betriebsausweis oder in der Kleidung von Arbeitnehmerinnen und Arbeitnehmern ist zumindest theoretisch ein Instrument der Überwachung und damit mitbestimmungspflichtig.

Grund genug sich mit dem Thema detaillierter auseinander zu setzen. Die vorliegende Broschüre informiert sowohl über die technischen Möglichkeiten von RFID-Systemen als auch über datenschutzrechtliche Implikationen und über Handlungsoptionen für BetriebsrätInnen die mit dieser Technologie konfrontiert werden.

Woltgang Katzian
Vorsitzender

Inhaltsverzeichnis

1. Was ist RFID? - Eine kurze Einführung in die Radiofrequenz-Identifikation 7
1.1. Der RFID-Chip 7
1.2. So funktioniert´s 7
1.3. Technische Merkmale 8
1.4. Der Chip ist unverwüstlich 8
1.5. Passive und aktive Transponder 9
1.6. Form, Größe, Reichweite der RFID-Chips 9
1.7. Lesegeräte und Lesereichweite 9
1.8. Risiken und Chancen 10
1.9. Anforderungen an den Datenschutz 11
1.10. Technische Sicherheitsrisiken 12
1.11. Electronic Product Code (EPC) 12
1.12. Zukunftsaussichten 12

2. Krieg und Frieden – RFID gibt es für alle Lebensbereiche 14
2.1. Am Anfang war das Militär 14
2.2. Wo liegen Möglichkeiten und Grenzen? 15
2.3. Unterschiedliche Systeme und ihre Einsatzbereiche 15
2.4. Energieversorgung 15
2.5. Datenübertragung 16
2.6. Frequenzbereiche und Reichweiten 16

3. RFID-Anwendungen heute 19
3.1. Anlagenverwaltung/Facility Management 19
3.2. Fertigung in der Industrie 19
3.3. Elektronische Wegfahrsperre 20
3.4. Öffentlicher Personennahverkehr 20
3.5. Tierhaltung 21
3.6. RFID-Implantate 21
3.7. RFID-Sensoren 22
3.8. e-Reise-Pass 22
3.9. Bibliotheken 25
3.10. Lager 25
3.11. Logistik 26
3.12. Tickets zur Fußball-WM 27
3.13. e-card: Die österreichische Gesundheitskarte 27

4. Im Handel hat die Zukunft bereits begonnen 30
4.1. Zukunftsszenario: Einkaufen 31
4.2. Pilotversuche im Handel 31
4.3. Vorreiter Metro und Rewe 32
4.4. Jedes Stück ist markiert 32
4.5. Vorsicht ist gut - Kontrolle ist besser 33
4.6. Rationalisierung versus Arbeitsplätze 34
4.7. Geht´s der Wirtschaft gut 34

5. RFID-Anwendungen morgen 36
5.1. Polymer-Technik 36
5.2. UHF-Transponder 36
5.3. Lokalisierung 36

5.4. Erfassen von Personen 37
5.5. Kombination mit biometrischen Verfahren 37
5.6. Kennzeichnen von Produkten und Gegenständen 37
5.7. Kriminalität 37
5.8. Personalausweise 37
5.9. Neue Formen bargeldlosen Bezahlens 38
5.10. Sicher in Krankenhäusern 38
5.11. Leistung im Sport messen 38
5.12. Organisation der Abfallentsorgung 38
5.13. Service an öffentlichen Plätzen 38
5.14. Intelligente Haushaltsgeräte 39
5.15. eGK: Die elektronische Gesundheitskarte der BRD 39
5.16. ELENA – Die Job-Card der BRD mit dem Namen einer griechische Göttin 40
5.17. Die Medaille hat zwei Seiten 42
5.18. Bei bester Gesundheit 43
5.19. Hemmnisse der RFID-Technik 44

6. Handlungsspielräume für BetriebsrätInnen 45
6.1. Persönlichkeitsrechte in Gefahr 45
6.2. Rechte der Beschäftigten im Arbeitsverhältnis 45
6.3. Betriebe wandeln sich 46
6.4. Der globalisierte Handel 46
6.5. Es liegt in des Hand des Betriebsrats 47
6.6. Personaldaten 48
6.7. Gesundheitsbelange 49
6.8. Planung Technischer Anlagen 50
6.9. Begleitende Kontrolle 50
6.10. Transparentes Verfahren 50
6.11. Datenschutzkonzept 51
6.12. Betriebsvereinbarung 51
6.13. Ergonomie 51
6.14. Qualifikation und Einschulung 52
6.15. Checkliste für den Betriebsrat 54

7. Rasterfahndung an der Kasse – Loss Prevention 55
7.1. Data Mining – Wie ihre Daten unterminiert werden 55
7.2. Das Fahndungsnetz der Supermarktketten 55
7.3. Kontrolle des Arbeitsverhaltens 56
7.4. Im Dauerkontakt mit dem Arbeitgeber 56
7.5. An der elektronischen Leine 56
7.6. Arbeiten im Galopp 57
7.7. Geofence-Technik 57
7.8. Pick-by-voice 58
7.9. Personenprofile 58
7.10. Vor Missbrauch nicht gefeit 59
7.11. Konsumentenschutz 59
7.12. Datendiebstahl 61
7.13. Kein Konsum ohne Datenschutz 61

8. Technische Analyse RFID-bezogener Angstszenarien 62
8.1. Unautorisierte Erfassung von Besitz 62
8.2. Tracking von Personen 63
8.3. Erheben sozialer Netzwerke 65
8.4. Personen für Objekte verantwortlich machen 67

9. RFID und Kryptographie (Verschlüsselung) 68
9.1. Kryptographische Methoden auf RFID-Systemen 68
9.2. Bedrohungsanalyse 68
9.3. Kryptographische Verfahren 68
9.4. Datensicherheit in der Praxis 71
9.5. Der RFID-Guardian – Anti-RFID-Gerät warnt vor Datendieben 71

10. RFID in der Kritik 72
10.1. RFID – eine Gefährdung der Privatsphäre mit neuer Qualität 72
10.2. Welche Folgen hat das 72
10.3. Forderungen zu RFID 73
10.4. Fazit 74

1. WAS IST RFID?

Eine kurze Einführung in die Radiofrequenz-Identifikation

RFIDs sind zweifellos eine zukunftsweisende Technologie. Funk-Etiketten kennt man seit dem II. Weltkrieg, wo sie zur Freund-Feind-Erkennung von Flugzeugen entwickelt wurden. Die Ahnen der heutigen RFID-Chips konnten ein Bit übertragen und waren klobig im Vergleich zu den heute gebräuchlichen hauchdünnen Folien.

Die Produkt- und Dienstleistungsbereiche, in denen sie sich einsetzen lassen, wachsen ständig. Und sie sind eine Technologie mit weltweiter Bedeutung. Die Republik Korea (Südkorea) machte im Jahr 2004 Inlandsumsätze mit RFID und hierauf bezogenen Geräten und Dienstleistungen von ca. 86,9 Mio. Euro. In Mexiko implantiert die Staatsanwaltschaft ihren Mitarbeiterinnen und Mitarbeitern einen VeriChip für den sicheren Zugang zu einem zentralisierten neuen Datenzentrum zur Verbrechensbekämpfung. In den USA schlägt Applied Digital Chef Scott Silverman vor, mexikanischen Arbeitsimmigranten – selbstverständlich freiwillig – ebenfalls einen solchen Chip in den Arm zu pflanzen, wohl als probates Mittel zur Bekämpfung des Terrors und der illegalen Einwanderung. Die Münchner Stadtbibliothek stattet alle Bücher und Medien mit RFIDs aus, damit ihre Ausleiher sich in Zukunft selbst bedienen können.

RFID ist die Abkürzung für Radio Frequency IDentification, also für Funk-Frequenz-Identifizierung, oder anders: Identifizierung per Funksignal.

1.1. Der RFID-Chip

Ein RFID-Chip (oder Tag) besteht aus einem klitzekleinen Chip mit Drähten, die eine Antenne bilden. Die Chips sind in Gegenstände, Etiketten oder Verpackungen eingebaut und brauchen keine eigene Batterie. Sie funktionieren per Funk (für Physik-Fans: per Induktion): Ein Lesegerät, häufig auch »Antenne« genannt, sendet einen Funk-Impuls und der Schnüffelchip sendet eine auf ihm gespeicherte weltweit einmalige Nummer zurück.

1.2. So funktioniert´s

Unsere Sinne können elektromagnetische Wellen nicht wahrnehmen, wir können sie weder riechen, noch hören, sehen oder fühlen. Das mag ein Grund dafür sein, dass sich viele Menschen für die kleinen Funkchips überhaupt nicht interessieren. Ein RFID-Chip sendet Information, ein Lesegerät liest sie und wir merken nichts davon. Auf welchen Frequenzen ein RFID sendet entscheidet über seine Reichweite und damit seinen möglichen Einsatz. Es nutzt vielleicht den Radiowellenbereich, der zwischen 30 kHz und 300 MHz liegt, aber es gibt auch RFIDs im Mikrowellenbereich. Viele Systeme für die Identifikation (beispielsweise Zugangskontrolle, Zeiterfassung, elektronische Wegfahrsperren) arbeiten bei 125 kHz, sie haben zwar eine relativ geringe Lesegeschwindigkeit, sind dafür aber billig. RFID-Chips im Einzelhandel nutzen meist 13,56 MHz, Lösungen in der Logistik den UHF-Bereich (868MHz, 915MHz sowie 2,45GHz). Für Industrielle, wissenschaftliche (Scientifical) oder Medizinische Anwendungen gilt der ISMBereich 2,4 bis 5 GHz.

Im Mikrowellenbereich funktionieren neben RFIDs auch Wireless LAN-Systeme (WLAN). Längere Wellen mit niedrigeren Frequenzen durchdringen viele Stoffe, brauchen also keinen Sichtkontakt, sie werden aber von Metall reflektiert. Für hohe Frequenzen kann schon Wasser ein Hindernis sein.

Weil RFIDs auf Produkte geklebt werden können, heißen sie auch Funk-Etiketten oder Labels. Sie können mehr Information speichern als die herkömmlichen Strichcodes, und anders als diese müssen sie nicht mehr optisch gelesen werden. So lassen sich die Einzelteile etikettieren und anschließend in einen Karton verpacken, das Lesegerät sieht durch die Umverpackung.

Für die Logistik sind sie deshalb ideal, denn ein Produkt lässt sich auf dem Transportweg verfolgen. Raffiniertere Chips können im Produktionsprozess steuern, was mit dem Bauteil passiert, auf dem sie angebracht sind.

RFIDs können also ein Objekt, ein Tier oder einen Menschen kennzeichnen, einen Prozess steuern und sie können Objekte oder Lebewesen lokalisieren. Hinter den RFID-Chips und Lesegeräten gehört dazu eine großräumige IKT-Infrastruktur für die vielen Anwendungen, Datenbanken zum Speichern der Produktcodes, ein Lokalisierungssystem wie GPS (Global Positioning System) zur Ortsbestimmung, Standards, Logistikverfahren oder Anwendungen im Warenwirtschafts- oder ERP-Bereich (Enterprise Resource-Planning).

Wo ein Chip eingesetzt werden soll ist ausschlaggebend dafür, ob der Chip selbst eine Energiequelle in Form einer Batterie hat (aktiv) oder auf die Energie angewiesen ist, die ihm das Lesegerät übermittelt (passiv). Passive RFIDs lassen sich nur lesen und nicht beschreiben, aktive lassen sich meist auch beschreiben, sie können weiter senden und haben mehr Speicherplatz. Ihre Batterien halten mehrere Jahre lang. RFIDs können sehr unterschiedliche Speicherkapazitäten haben, und sie können mit einem eigenen Prozessor ausgestattet sein, der beispielsweise Daten verschlüsselt. Je leistungsfähiger ein Chip ist, umso teurer wird er natürlich.

Beim klassischen Scannen muss der Scanner durch den/die Kassierer/-in im Supermarkt, den/die Lagerarbeiter/-in in der Warenannahme per Hand auf die jeweiligen Strichcodes ausgerichtet werden. RFID als Funktechnik ermöglicht hingegen, im Unterschied zum Lichtscanner, die automatische Erfassung und Identifikation der Ware. Bei RFID ist jede Ware, jedes Produkt mit einem so genannten Transponder (RFID-Chip, RFID-Tag) versehen. Die Ware wird nun einfach an einem Lesegerät vorbeigeführt und Funkwellen übertragen, die im RFID-Chip gespeicherten Informationen. So können einzelne Produkte, Kartons oder ganze Paletten mit einem Tag versehen werden. Lese-Tore entlang der gesamten Supply-Chain – vom Fabrikstor des Herstellers bis zum Regal des Supermarktes – ermöglichen den gesamten Warenweg nach zu verfolgen. Funk-Etiketten kennt man seit dem II. Weltkrieg, wo sie zur Freund-Feind-Erkennung von Flugzeugen entwickelt wurden. Die Ahnen der heutigen RFID-Chips konnten ein Bit übertragen und waren klobig im Vergleich zu den heute gebräuchlichen hauchdünnen Folien.

1.3. Technische Merkmale

Ein RFID-System besteht aus drei Komponenten:

1. **Dem Transponder als Datenträger, auch RFID-Chip oder RFID-Tag, RFID-Label und Funketikett genannt.**

2. **Einer Sende-Empfangs-Komponente, auch als Reader bezeichnet**

3. **Der Integration mit anderen Systemen, wie Servern, einem Data-Warehouse oder zB einem Kassensystem**

Der RFID-Chip besteht aus einer Antenne, dem Chip auf dem die Daten gespeichert werden und einer Schaltung, die diese beiden Komponenten verbindet. Chip und Antenne sind auf eine Spezialfolie appliziert. Dieses Inlay, der eigentliche Chip wird dann auf unterschiedlichen Trägern angebracht.

1.4. Der Chip ist unverwüstlich…

Die Gestaltung und Bauform der Chips richtet sich nach den Einsatzgebieten, je nach dem in welchen Träger sie integriert werden sollen und welchen Umweltbedingungen wie Schmutz, Hitze oder Feuchtigkeit sie standhalten sollen. Es gibt Chips, die resistent gegen solche Umgebungsbedingungen sind. Die Bauform der Transponder reicht von der Form von Nägeln, die in Paletten eingeschlagen werden können bis zu hauchdünnen Papierfolien, die auf den Träger geklebt werden. Glastransponder in der Form kleiner Stäbchen werden meist unter die Haut von Tieren und mittlerweile auch Menschen injiziert und dienen ebenfalls der Identifikation. Chipcoins in der Form von Münzen werden in Parkhäusern eingesetzt und runde Button-Tags mit einem Loch in der Mitte können an Träger angeschraubt werden. Auf Grund hoher Produktionskosten wird laufend versucht die Chips in der Herstellung billiger zu machen. Die letzte Entwicklung auf diesem Gebiet ist der Versuch RFID-Chips zu drucken. Dabei wird die Polymerelektronik (Polymere: auf sehr dünne Polyesterfolien in mehreren Schichten aufgedruckt. Diese gedruckten Chips haben zwar nur eine Speicherkapazität von bis zu 128 Bit, sind jedoch von den Herstellungskosten ungleich billiger als die derzeitigen Transponder.

1.5. Passive und aktive Transponder

RFID-Chips können in aktive und passive Transponder unterschieden werden. Aktive Transponder besitzen eine eigene Energiequelle (Batterie) um Lesedistanzen von einigen Metern überbrücken zu können. Sie können gelesen, aber auch beschrieben werden und verfügen durch ihre Energiequelle über eine höhere Sendereichweite als auch über eine größere Speicherkapazität und sind natürlich teurer als passive Transponder. Passive Transponder verfügen somit über keine eigene Energieversorgung. Passive Transponder beziehen ihre Energie zur Übertragung der Informationen von den empfangenen Funkwellen aus dem Lesegerät. Durch ihre geringere Speicherkapazität werden sie benutzt um eine eindeutige Identifikationsnummer zu speichern, den Electronic Product Code (EPC). Passive Transponder benötigen zwar eine leistungsfähigere Leseeinheit, haben aber eine sehr lange Lebensdauer und weitaus geringere Herstellungskosten als aktive Transponder.

Ein Data-Warehouse bzw. Datenlager ist eine zentrale Datensammlung (meist eine Datenbank), deren Inhalt sich aus Daten unterschiedlicher Quellen zusammensetzt. Die Daten werden von den Datenquellen in das Data-Warehouse geladen und dort vor allem für die Datenanalyse und zur betriebswirtschaftlichen Entscheidungshilfe in Unternehmen langfristig gespeichert. Der Begriff stammt aus dem Informationsmanagement in der Betriebswirtschaft. Ein Data-Warehouse dient der Informationsintegration.

1.6. Form, Größe, Reichweite der RFID-Chips

RFID-Chips sehen sehr unterschiedlich aus, winzig klein wie ein Stecknadelkopf oder fast so groß wie ein Taschenbuch, rund oder eckig, mit sichtbarer oder unsichtbarer Antenne, ... Sie haben verschiedene Namen: Transponder (transmitting responder), Tag oder Label. RFIDs lassen sich auch abschalten, dauerhaft oder auf Zeit. IBM entwickelt zur Zeit einen Chip, dessen Antenne sich abknipsen lässt, es kann aber auch eine Kill-Funktion eingebaut sein, oder Sie können den Chip in die Mikrowelle legen. Größe und Form der RFID-Chips hängen von der benötigten Antenne ab, deren Typ wiederum von der Frequenz auf der gesendet werden soll abhängig ist. Für größere Distanzen von mehreren Metern, wie oben beschrieben, sind aktive Transponder erforderlich. Durch ihre eingebaute Batterie ist auch ihre Bauweise größer. So können RFID-Chips je nach Einsatzgebiet und benutzter Technik die Größe von hauchdünnen Folien bis zum Format von Büchern annehmen. Bei geringen Reichweiten wie im Lebensmitteleinzelhandel oder Bekleidungseinzelhandel wo die Etiketten direkt am Produkt angebracht werden sind dadurch passive Transponder mit geringen Reichweiten ausreichend. Hingegen sind bei der Erfassung der gesamten Ladung von LKWs größere Reichweiten zu überbrücken, um die gesamte Ladung einlesen zu können.

Die Kosten der RFID-Chips hängen, wie oben beschrieben, von der Art (aktive oder passive), von der benötigten Stückzahl und davon ob es sich um Einweg- oder Mehrwegchips handelt ab. Passive RFID-Chips kosten bei einer Abnahmemenge von einer bis zehn Milliarden pro Stück zwischen fünf und zehn Cent. Bei einer kleineren Auflage von ca. 10.000 Stück beläuft sich der Stückpreis zwischen fünfzig Cent und einem Euro.

1.7. Lesegeräte und Lesereichweite

Es wird unterschieden zwischen fix montierten und mobilen Lesegeräten, auch Terminals oder Handlesegeräte genannt. Auch hier ist die Größe und Bauform vom Einsatz abhängig. Will man ganze Paletten auf einem LKW oder viele mit RFID-TAGS versehene Produkte auf einmal (genannt: Pulkerfassung) erfassen, werden eher so genannte Tunnelscanner zum Einsatz kommen. Der LKW oder der Einkaufswagen im Lebensmitteleinzelhandel rollen dann durch diese bogenförmigen Tunnelscanner.

Die Lesereichweite der RFID-Chips ist abhängig von der eingesetzten Funkfrequenz, der Antennengröße und den Umweltbedingungen. Wie bereits erwähnt bewegen sich die Reichweiten bei passiven Chips daher zwischen einigen Zentimetern bis zu zehn Metern. Aktive RFID-Tags können Reichweiten von bis zu hundert Metern erzielen.

1.8. Risiken und Chancen

Zugangskontrollen sind ein beliebter Einsatzzweck für die Chips, sowohl in Bereichen, in denen Sicherheit wichtig ist, wie Atomkraftwerken, Flughäfen oder Rechenzentren, als auch beim wenig sicherheitskritischen Benutzen des öffentlichen Nahverkehrs. Dort wird die Karte eingesetzt, um Fahrtkosten abzubuchen. Das alles spart Zeit, ist bequem und scheint sicher zu sein. Nur schade, dass der neue Reisepass so viel teurer ist als der alte. Vielleicht sparen Sie das aber wieder ein, wenn Ihr kommunales Nahverkehrssystem automatisch den für Ihre Nutzung günstigsten Tarif abrechnet? Schon jetzt ist in manchen Städten der Busfahrschein aus dem Automaten billiger als der beim Fahrer oder am Schalter gekaufte. Das lässt sich sehr wohl auch als Preisdiskriminierung derjenigen kritisieren, die keine Möglichkeit (oder nicht den Wunsch) haben, diesen Weg zum Erwerb einzuschlagen.

Auch andere Dienstleistungen werden wohl billiger werden, jedenfalls für die Anbieter, wenn weniger Aufwand für eine menschliche Bearbeitung anfällt. Manche Reisepässe enthalten bereits einen RFID-Chip, der übrigens mitsamt den Daten schon geklont werden konnte, für die Personalausweise wird darüber diskutiert. Andere Länder sind wesentlich weiter im Einsatz, so soll China zur Zeit seine Personalausweise und Führerscheine auf RFID-Technik umstellen, in den USA sollen es im ersten Jahr 67 Millionen Pässe werden, und weltweit wird ein jährliches Marktvolumen für Ausweispapiere von 125 Millionen erwartet.

Hier treffen mehrere gesellschaftliche Trends zusammen:

Der Wunsch nach möglichst umfassender Sicherheit und der nach mehr Komfort, vielleicht auch ein Streben staatlicher Einrichtungen nach mehr Kontrolle über die Bevölkerung. Die Kombination von berührungslos auslesbaren Ortungs- und Identifizierungsdaten, Videoüberwachung und einer Vorratsspeicherung von Kommunikationsdaten auf der einen (staatlichen), und von steigenden Komfortwünschen, Zeitersparnis und Rationalisierungsbestrebungen auf der anderen (privatwirtschaftlichen) Seite sollte die Gesellschaft beschäftigen. Diese Entwicklung bedeutet in Zukunft neue Herausforderungen für diejenigen, denen es wichtig ist selbst zu entscheiden, wer was über sie oder ihn erfährt. Immerhin ist das ein verfassungsrechtlich garantierter Anspruch.

Die Chancen der Rationalisierung werden von der Industrie deutlich wahrgenommen und sie sind im Sinne der Wettbewerbsfähigkeit und Ressourcen-Ersparnis sicher wichtig. Die Kehrseite jeder Rationalisierung ist aber der Verlust von Arbeitsplätzen, und es wundert doch, dass dieses Thema so gut wie gar nicht in der öffentlichen Diskussion auftaucht. Wenn doch einmal, wird beschwichtigt, dass eingespartes Personal für höher qualifizierte Tätigkeiten eingesetzt werden soll. Wenn es um Fragen der Technik geht, die eine Entscheidung verlangen zwischen einem Implantat oder einem tragbaren Chip, fällt sicher die Abneigung vieler Menschen gegenüber einem eingepflanzten Fremdkörper ins Gewicht. Das Armband oder der Anhänger können zwar verloren gehen oder vertauscht werden, aber der Chip unter der Haut kann wandern. Wenn das flotte Implantat für den Disko-Besuch oder den Zugang zum PC unter wenig hygienischen Bedingungen injiziert wird, können hässliche Entzündungen folgen, wie bei Piercings auch.

RFID-Chips kommunizieren mit Schreib-/Lesegeräten durch elektromagnetische Wellen. Von denen sind wir ohnehin umgeben, die meisten kommen von drahtlos kommunizierenden Geräten (beispielsweise im Mobilfunk oder den Netzen rund um den PC im Büro oder Haushalt), aber auch von jedem Elektrogerät im Betrieb. Es ist noch völlig ungeklärt, wie sich eine weitere Zunahme des allgegenwärtigen Elektrosmogs auswirken wird. Dass elektromagnetische Wellen einen Einfluss auf den menschlichen Körper haben, steht außer Frage. Dabei ist nicht nur der Wärme-Effekt zu diskutieren, sondern auch gentoxische Wirkungen in den Körperzellen. Die EU-weite REFLEX-Studie hat den Zusammenhang zwischen einer Radiowellen-Exposition und der Entstehung funktioneller Störungen zwar nicht belegt, die Annahme aber plausibler gemacht. Träger von Hörgeräten und Herzschrittmachern sollten jedenfalls Abstand von Schreib-/Lesegeräten halten.

Zwar gibt es auf europäischer Ebene bereits gesetzliche Regelungen zum Gesundheitsschutz für die Öffentlichkeit und am Arbeitsplatz, auf diesem Gebiet ist aber weitere Forschung nötig. Auch sind wohl Probleme zu erwarten, wenn private Unternehmen oder der Staat auf personenbezogene Daten zugreifen wollen und können, die wir alle lieber für uns behalten möchten.

Inzwischen hat es sich herumgesprochen, dass RFIDs datenschutzrechtlich alles andere als unbedenklich sind.

1.9. Anforderungen an den Datenschutz

Vor allem in der Fähigkeit, Personen zu lokalisieren, liegt etwas Beunruhigendes. Schließlich ist es nicht schwierig, ein Objekt mit einer Person in Verbindung zu bringen. Wer mit der Kunden- oder Geldkarte einkauft und dann ein RFID-gekennzeichnetes Objekt aus dem Laden trägt, der lässt sich womöglich auch an einem anderen Ort unbemerkt identifizieren. Bei den Strichcodes, die Sie heute noch auf fast allen Etiketten im Einzelhandel finden, ist das nicht möglich.

Der Bundesbeauftragte der BRD für den Datenschutz, Peter Schaar, verlangt, dass der RFID-Einsatz dem Verbraucher bekannt sein muss und nicht heimlich erfolgen darf. Daten der Chips aus verschiedenen Produkten dürfen nicht zu Verhaltens-, Nutzungs- und Bewegungsprofilen zusammengeführt werden, und die Verbraucher müssen die Möglichkeit haben, den Speicherinhalt auszulesen. Die Kunden sollen die RFIDs auf Produkten und Verpackungen deaktivieren und die Lese-/Schreib-Mechanismen kontrollieren können. Im Sinne eines effektiven Datenschutzes sollten die Betroffenen möglichst früh informiert werden, also bereits auf dem Produkt und an den Verkaufsregalen, und nicht erst, wenn die Daten des Kunden durch ein Kassensystem erfasst werden. Schaar schlägt vor, dass sich Industrie und Handel über Selbstregulierung und Selbstverpflichtung zur umfassenden Gewährleistung des Datenschutzes verpflichten.

So haben auch die Initiatoren des BigBrother-Awards, in einem Positionspapier Forderungen aufgeführt, die von einer Vielzahl von Bürgerrechts-Organisationen unterstützt werden. Sie halten freiwillige Selbstverpflichtungen nicht für ausreichend und verlangen eine Technikfolgen-Abschätzung und bis zu deren Ergebnis die Einhaltung folgender Grundregeln durch die Hersteller und Anwender von RFIDs:

- Chips und Lesegeräte müssen deutlich und verständlich gekennzeichnet sein, auch mit ihren technischen Spezifikationen.

- Jeder Lesevorgang muss für die Verbraucher erkennbar sein, und die Zwecke bekannt gegeben werden, für die die Daten ausgelesen werden. Nur die notwendigen Daten für diesen jeweiligen Zweck dürfen erfasst werden.

- Niemand darf genötigt oder gezwungen werden, RFIDs zu akzeptieren.

- Die Übermittlung der Daten muss sicher und geheim sein, eine neutrale Instanz mit der Kontrolle beauftragt werden. Es muss eine verpflichtende Verantwortlichkeit der Anwender geschaffen werden, und bei öffentlichen und privatwirtschaftlichen Einrichtungen eine Instanz, an die sich die Bürgerinnen und Bürger bei Verletzungen ihrer Rechte wenden können.

- Die Chips dürfen nicht als Mittel eingesetzt werden, das die Anonymität einer Person verringert oder unmöglich macht. Menschen dürfen nicht mit Hilfe der RFIDs verfolgt werden, es sei denn, sie hätten ausdrücklich und schriftlich zugestimmt.

Von dieser Situation sind wir freilich noch weit entfernt, auch wenn viele Unternehmen sich darüber im Klaren sind, dass ein guter Schutz der Verbraucher der Technik den Weg ebnen kann. Der wenig verbraucherfreundliche Umgang einiger Unternehmen mit RFIDs hat schon viele Menschen misstrauisch gemacht. –

Es sind noch viele Fragen offen:

- Werden Ihnen aus dem Deaktivieren eines RFIDs Nachteile entstehen?

- Können Sie das Produkt nach geltendem Verbraucherschutzrecht dann noch umtauschen oder zurückgeben?

- Wie ließe sich ein Chip verlässlich deaktivieren, der in ein Gerät integriert ist?

- Was bedeutet es, Millionen kleiner, schwer auffindbarer Chips umweltgerecht zu entsorgen?

Auf diese Fragen kann auch unsere Broschüre noch keine Antwort geben, auf viele andere aber hoffentlich doch.

1.10. Technische Sicherheitsrisiken

Es sind auch hier wie auf ihrem Computer die Viren. Forschern der Universität Amsterdam ist es bereits gelungen einen Virus für einen RFID-Chip zu entwickeln. Die Computerviren können in RFID-Chips eingeschleust werden. Von dort wäre es möglich, dass die Viren ihren Weg in die Software der Lesegeräte und der damit verbundenen Datenbanken finden. Wie Wissenschafter dem Medium Telepolis (http://www.telepolis.de) berichteten, könnten die Viren durch das Scannen eines infizierten Chips in die Datenbanken von Warenwirtschaftssystemen eindringen.

Gesamte Systeme ließen sich so manipulieren. Reisegepäck auf Flughäfen könnte in die falschen Flugzeuge verladen werden. LKW-Ladungen großer Handelsketten könnten in die falschen Filialen dirigiert werden oder Kaufpreise von Waren in Kaufhäusern könnten gefälscht werden. So wären bei einem Virusbefall eines Systems auch wichtige Informationen, die auf dem Chip gespeichert sind, wie Echtheitszertifikate oder die Angabe des Ursprungslandes vor Fälschung nicht mehr sicher.

1.11. Electronic Product Code (EPC)

EPC ist die Norm bzw. der Standard nach dem weltweit die eindeutigen Seriennummern der RFID-Chips vergeben werden. Der EPC ermöglicht es jedes auf der Welt hergestellte Produkt eindeutig zu identifizieren. Dadurch wird jede Flasche Bier, jeder Mantel oder jede Milchpackung, die auf der Welt hergestellt werden zum Unikat. Von Beginn der Herstellung bis zum Konsum beim Endverbraucher kann der Lebensweg jedes einzelnen Produktes nachvollzogen werden. Mit dem internationalen Electronic Product Code (EPC) erhält jeder Chip eine weltweit eindeutige Identifikationsnummer. Es gibt Varianten mit 64 Bit (EPC-64), 96 Bit (EPC-96) und 256 Bit (EPC-256). Neben anderen Informationen enthält beispielsweise der EPC-96 die Seriennummer des Chips (36 Bit) und mit einer Gesamtlänge von 44 Bits sowohl eine Nummer für den Hersteller (20-40 Bits) als auch für die Produktart, die der Chip kennzeichnet, den Item- oder Objektcode (4-24 Bit).

Mittlerweile hat die Standardisierungsorganisation »EPCglobal Inc.« (http://www.epcglobal.de) bereits eine Weiterentwicklung des EPC vorgestellt. Die neue Generation des EPC wird »EPC Gen 2« genannt. »Gen 2« arbeitet im Bereich der Ultrahochfrequenz (UHF), bietet mehr Informationen und ist weltweit einsetzbar. Ziel dieses neuen Standards ist es globale Kompatibilität, Schreib- und Lesefähigkeiten sowie die Adaptionsmöglichkeiten an zukünftige EPC-Klassen zu ermöglichen. Die zweite Generation »EPC Gen 2« verfügt bereits über ein größeres Speichervolumen, eine bessere Security-Verschlüsselung der Etikettendaten, offene Standards für Bezugsquellen von Etiketten (dadurch können Etiketten verschiedener Anbieter kombiniert werden) und höhere Leseraten. Für den Einsatz der Chips der »Gen 2« sind jedoch eine eigene Lesehardware und spezielle Speicherchips erforderlich.

Der Elektronische Produktcode (EPC), in Zusammenarbeit zwischen den Auto-ID Labs und EPCglobal entwickelt, ermöglicht eine eindeutige Kennzeichnung von Objekten (zB Handelseinheiten, logistische Einheiten oder Transportbehälter). Dafür wird der EPC auf einem Datenträger gespeichert welches im Anschluss an ein Objekt angebracht wird. Als Datenträger wird in der Regel ein RFID-Chip verwendet, da dieser Code dafür entwickelt wurde. Der EAN128-Barcode bietet ähnliche Kennzeichnungsmöglichkeiten.

1.12. Zukunftsaussichten

Die Einschätzungen bezüglich des zukünftigen Einsatzes von RFID sind noch sehr inhomogen. Es muss auch darauf hingewiesen werden, dass die hier wiedergegebenen Marktanalysen und zitierten Szenarien vor dem Jahre 2008 und seiner wirtschaftlichen Situation vorgestellt wurden. Dennoch ist RFID, nicht nur aufgrund sich darbietender Rationaliserungsmöglichkeiten, ein Zukunftsmarkt.

»Deutsche Bank Research« geht davon aus, dass das Volumen des gesamten weltweiten RFID-Marktes mittelfristig um 57% pro Jahr zunimmt. Die Analysten/-innen des Finanzinstitutes schätzen, dass sich der Markt von derzeit ca. zwei Milliarden Euro auf 22 Milliarden Euro im Jahr 2010 ausdehnen wird. Das Marktforschungsunternehmen »ID-TechEx« beziffert den globalen Markt für RFID – inklusive Tags, Systemen und Dienstleistungen im Jahr derzeit auf ca. 2 Milliarden US-Dollar. Für das Jahr 2010 erwarten sie ein Volumen von 12,35 Milliarden. Bis zum Jahre 2005 wurden weltweit 1,8 Milliarden RFID-Tags verkauft. Bis 2010 wird vor allem ein Wachstum für Chips zur Applikation an Paletten erwartet. Im Jahre 2005 waren es 0,4

Milliarden Stück für die Auszeichnung von Paletten (genannt: Unit-Tagging), 2010 soll die Zahl auf 30 Milliarden anwachsen und dann 2015 35 Milliarden erreichen.

Noch größeres Wachstumspotenzial erwartet man sich im so genannten Item-Tagging, das vor allem bei der Kennzeichnung von Gepäckstücken, Tieren, Büchern, Arzneimitteln und Tickets Verwendung findet. Waren es im Jahr 2005 0,5 Milliarden Stück, beläuft sich die Schätzung für 2010 auf 27 Milliarden und für 2015 auf eine Billion. Die Umsätze im Marktsegment der RFID-Technologie beliefen sich im Jahr 2007 auf geschätzte 1,1 Milliarden US-Dollar. Großbritannien und die BRD liegen mit einem gemeinsamen Marktanteil von 40% an der Spitze. Momentan konzentriert sich der Markt vor allem auf Tags in den Bereichen der Paletten und Verpackungen, doch wird in diesem Marktsegment bereits für 2008 eine Sättigung erwartet.

Zum Abschluss noch eine Prognose von Soreon Research: Laut dieser Analyse werden die RFID-Tags einen Anteil von rund 75% des gesamten RFID-Markts ausmachen. Soreon Research geht von einem deutlich überwiegenden Anteil an passiven Tags aus. Die Hersteller selbst prognostizieren eine Prozentverteilung von 71% zu 29% für passive Tags.

Der Einzug von RFID in die Kassiervorgänge des Einzelhandels wird noch dauern, da jedes einzelne Produkt, auch wenn es nur wenige Cent kostet, einen Chip benötigen würde. Momentan ist es noch nicht möglich Chips zu rentablen Kosten für alle Produkte zu produzieren. Doch bietet, die oben erwähnte Polymertechnik, möglicherweise in der Zukunft die Möglichkeit preisgünstigere Chips zu drucken. So genannte „Future Stores“ mit RFID-Kassensystemen werden zwar schon von Handelsketten (Metro, Rewe) zur Erprobung geführt. Eine generelle Umstellung aller Filialen ist aber aus den erwähnten Gründen noch Zukunftsmusik.

Auch die Möglichkeit ein Produkt mit einem weltweit lesbaren Tag zu versehen ist noch nicht realisierbar. Einzelne Versuche sind schon in Erprobung, beschränken sich aber noch auf einzelne Geschäftskontakte. Ein weltweiter Einheitsstandard ist noch in der Entwicklungsphase. Auf technischer Seite gibt es noch Probleme beim Lesen der Daten. So stellen metallische Oberflächen oder Flüssigkeiten noch Hindernisse beim Auslesen der Daten auf den RFID-Chip dar. Ebenso ist die bereits erwähnte Gefahr von Infektion durch Viren oder die Frage, wie sich die auf dem RFID-Tag ausgelesenen Daten sicher vor Manipulation auf das Lesegerät übertragen lassen, noch nicht geklärt.

2. KRIEG UND FRIEDEN
RFID gibt es für alle Lebensbereiche

Es gibt sicher viele wünschenswerte Anwendungen für die Zukunft: So wäre eine Kennzeichnung von Bauteilen für elektronische Geräte beim Recycling hilfreich, RFIDs auf verschiedenen Produkten könnten sowohl die Fälschung (beispielsweise bei Arzneimitteln) als auch den Diebstahl teurer Güter (Kennzeichnung von Elektronikgeräten, Wegfahrsperre bei Fahrzeugen) erschweren. Garantie- und Rückgaberechte könnten im Chip festgeschrieben sein, Rückrufaktionen erleichtert werden. Verbesserte Logistik-Abläufe können Energie sparen, RFIDs in Fertigungsprozessen den Ressourcen-Verbrauch minimieren. Produkte können zu ihrem Ursprung zurückverfolgt werden. Werden RFIDs mit Sensoren kombiniert, erleichtern sie die Qualitätskontrolle, beispielsweise bei Produkten, die ohne Unterbrechung in der Kühlkette verarbeitet oder transportiert werden müssen. Zahlreiche Einsatzmöglichkeiten tun sich in Labors auf, beispielsweise bei Gewebeproben für die Life Sciences.

2.1. Am Anfang war das Militär

Zum Einsatz auf manchen dieser Gebiete sind aber noch Schwierigkeiten zu überwinden. Sie sind einerseits technischer Art, wie die Wechselwirkungen zwischen hochfrequenten Feldern, liegen aber auch in den Standards. Die Standardisierungsbemühungen sind auf einem guten Weg, zumindest innerhalb der Europäischen Union. Die IT-Infrastruktur muss aber noch ausgebaut werden. Immerhin ist das Ziel, RFIDs durch Massenherstellung billiger zu machen, durch ihre zunehmende Verbreitung in den letzten Jahren deutlich näher gerückt.

Die Experten sehen auch im Gesundheitswesen ein wichtiges Einsatzgebiet, wenn beispielsweise im Krankenhaus der Zugang zu den Behandlungsdaten durch einen Chip im oder am Patienten erleichtert wird. Gebrechliche könnten bei Unfällen einen automatischen Notruf auslösen oder verwirrte Menschen könnten besser zu finden oder zu identifizieren sein. Selbstverständlich hat auch die Rüstungsindustrie die nützlichen Kleinteile im Blick. Sie sollen mit erweiterten Funktionen sogar in die Lage versetzt werden, Satelliten, Handy-Netze und WLAN-Hot-Spots anzufunken und ihren Standort mitzuteilen. Das haben sich die Militärlogistiker gewünscht.

Wie viele andere Techniken wurde übrigens auch die Transponder-Technik zunächst für militärische Zwecke entwickelt und erst 1977 für den zivilen Einsatz freigegeben. Pläne der europäischen Zentralbank, die Euro-Banknoten mit RFIDs zu versehen, scheinen sich zerschlagen zu haben. Davon hatte man sich erhofft, die Wege schwarzen Gelds verfolgen zu können, und die Chips sollten die Geldscheine fälschungssicherer machen.

Wie oben beschrieben gehören zu einem RFID-System Lesegeräte und die Etiketten (auch Tags, Labels, Transponder genannt), die auf Anstoß des Lesegerätes Signale mit einem programmierten oder programmierbaren Informationsgehalt abgeben. Da die Tags so weit miniaturisiert sind, dass sie in Objekte oder Verpackungen eingearbeitet werden können, werden sie als intelligente Etiketten (smart tags oder smart labels), Funkchips oder kurz Tags bezeichnet.

Wenn sie komplexe Signale abstrahlen können, wird auch die Bezeichnung Transponder (transmitting responder) verwendet. Informationen werden zwischen Lesegeräten und Tags mittels elektromagnetischer Wellen oder per Funk übertragen. Tags mit komplexerer Funktion brauchen Energie, sie wird normalerweise durch elektromagnetische Felder übertragen. Die Lesegeräte sind ihrerseits Teile eines umfangreicheren Systems. In der Regel sind sie an größere Softwareanwendungen und Datenbanken angeschlossen, damit die Daten weiterverarbeitet werden können.

So können mit RFID-Systemen beispielsweise aktueller Zustand und Standort eines Produkts schnell und genau festgestellt werden, wenn Prozesse in einem Unternehmen werksübergreifend organisiert werden müssen.

2.2. Wo liegen Möglichkeiten und Grenzen?

Die feld– oder funkbasierte Datenübertragung ist ein wesentlicher Vorteil der RFID-Technik gegenüber herkömmlichen Identifikationssystemen wie dem weit verbreiteten Barcode und dem von Postsendungen bekannten Datamatrix-Code, die optisch ausgelesen werden. Funk und Felder erweitern die Lesemöglichkeiten, deshalb lässt sich RFID auch überall dort einsetzen, wo Schmutz und ungünstige Objektpositionierung ein optisches Auslesen erschweren. RFID-Systeme ermöglichen die Identifikation der Tags und das Auslesen ihrer Daten innerhalb einer durch Sendeleistung und Empfangsempfindlichkeit begrenzten Reichweite. Mehrere intelligente Etiketten, beispielsweise auf Warenpaletten oder in Einkaufswagen, können in einem Vorgang angesprochen werden.

Dass RFID als Mittel zur berührungslosen Objekterkennung in den letzten Jahren rasant an Bedeutung gewinnt, ist nicht zuletzt dem technischen und technologischen Fortschritt auf diesem Gebiet zuzurechen. Die Optimierung der Fertigungstechnologie lässt Preis und Abmessungen schrumpfen. Gleichzeitig werden die in den Tags verwendeten Prozessoren leistungsstärker. Die Industrie findet immer neue Anwendungen für die Technik. Besonders in der Logistikbranche verbreitet sich RFID rasch.

Über den ökonomischen Nutzen hinaus entstehen mit zunehmender Verbreitung und Leistungsfähigkeit auch gesellschaftliche und persönliche Risiken aus der Möglichkeit, Personen und Objekte verdeckt zu identifizieren. Um sowohl die Risiken als auch die Möglichkeiten von RFID-Systemen einschätzen zu können, ist ein Einblick in ihre Technik und Leistungsmerkmale hilfreich, der aber immer nur eine Momentaufnahme sein kann. Die Technik hat die Grenzen ihrer Entwicklung noch lange nicht erreicht. Eine grobe Orientierung geben die Sende- und Empfangsentfernungen, die maßgeblich durch die verwendeten Frequenzen und die Übertragungsverfahren von Daten und Energie bestimmt werden.

2.3. Unterschiedliche Systeme und ihre Einsatzbereiche

Seit vielen Jahren gibt es elektronische Artikelsicherungssysteme (EAS) in Kaufhäusern. Sie haben nur eine geringe Leistungsfähigkeit, denn ihre Funktion ist darauf beschränkt, ein An-/Aus-Signal zu geben. Individuelle Objekte können mit ihnen nicht unterschieden werden.

In der Regel wird mit dem Begriff RFID jedoch mehr als nur der Diebstahlschutz assoziiert. Systeme mit mittlerer Leistungsfähigkeit können über Speicher von mehreren Kilobyte verfügen, die bei manchen Tag-Typen auch wieder beschreibbar sind. Hier sind solche Systeme anzusiedeln, die zur Objekt- bzw. Produkterkennung eine längere Identifikationsnummer an ein Lesegerät übermitteln. So lassen sich, anders als bei den EAS, individuelle Objekte aus derselben Produktreihe voneinander unterscheiden, was vom Warentransport vom Produzenten zum Laden bis zur Abrechnung an der Kasse genutzt werden kann. Je nach Einsatzgebiet können die Tags über Authentifizierungs- und Verschlüsselungsfunktionen verfügen.

RFID-Systeme mit hoher Leistungsfähigkeit zeichnen sich dadurch aus, dass die Prozessoren auf den Tags komplexe Berechnungen für Verschlüsselung und Authentifizierung ausführen können. Sie sind teurer und kommen deswegen vorwiegend in sicherheitsrelevanten Anwendungen zum Einsatz wie der Identifikation von Personen, Bezahlvorgängen und Zugangskontrollen.

2.4. Energieversorgung

RFID-Tags sind im einfachsten Fall mit einer Logikschaltung ausgerüstet, die die für die Informationsabgabe benötigte Datenfolge produziert. Tags der komplexeren Art besitzen sogar Prozessoren und Speicherbausteine. Logikschaltungen, Prozessoren und Speicher benötigen für die Aktivierung, Programmsteuerung und Datenübertragung eine Energieversorgung. Unterschieden wird zwischen aktiven und passiven RFID-Tags.

Aktive RFID-Tags verfügen über eine eigene Spannungsversorgung, zum Beispiel eine kleine Batterie. Sie versorgt den Prozessor, der von außen durch das Feld– oder Funksignal des Lesegeräts aktiviert wird. Wegen der Batterie sind aktive RFID-Tags meist größer als passive. Deshalb, und auch aus Kostengründen, werden sie nicht in der massenhaften Artikelkennzeichnung im Handel genutzt.

Passive RFID-Tags beziehen ihre Betriebsenergie aus dem elektromagnetischen Feld oder aus der elektromagnetischen Welle des Lesegerätes. Das Lesegerät kann einen in seiner Reichweite befindlichen Tag entweder permanent oder gepulst mit Energie versorgen. In gepulsten Systemen werden die Daten vom Lesegerät simultan mit der Betriebsenergie übermittelt.

Die Tags speichern die Energie in Kondensatoren, um die Versorgung in den Phasen zu sichern, in denen das Lesegerät die Energieübertragung zwecks Informationsempfang unterbricht.

2.5. Datenübertragung

Für die Datenübertragung zwischen Lesegeräten und RFID-Tags gibt es drei verschiedene Verfahren:

- die kapazitive Kopplung
- die induktive Kopplung (Transformator-Prinzip)
- und das Backscatter-Verfahren.

Bei einer kapazitiven Verbindung müssen die Tags so nahe am Lesegerät sein, dass der Plattenkondensator-Effekt zum Tragen kommt. Zwischen den Kondensatorflächen von Lesegerät und Tag wird ein elektrisches Feld aufgebaut. Die Logik des Tags verändert seine kapazitiven Eigenschaften in zeitlicher Folge. Diese wiederum beeinflussen den Feldverlauf, der Rückwirkungen auf das Lesegerät ausübt. Über diese Veränderungen können die gewünschten Informationen ausgelesen werden. Die Versorgungsenergie kann aus einem zusätzlichen elektromagnetischen Feld nach dem Transformator-Prinzip gewonnen werden. Induktiv gekoppelte Systeme arbeiten nach diesem Transformator-Prinzip. Das Lesegerät baut über seine Sendespule ein magnetisches Feld auf und versorgt die Tags über deren Empfangsspule mit Energie. Die Tags entziehen dem Feld Energie, beispielsweise durch eine Folge von Veränderungen des Widerstandswerts der Empfangsspule. Anhand dieser Änderungen ermittelt das Lesegerät die zu übertragenden Daten.

Beim Backscatter-Verfahren kommt ein aus der Radar-Technik bekannter Effekt zum Einsatz: Ein Objekt reflektiert elektromagnetische Wellen, wenn seine Ausdehnung mehr als die Hälfte der Wellenlänge des Signals beträgt. Dieser so genannte Rückstrahleffekt funktioniert besonders gut, wenn die Antennen der Tags Resonanz mit der Sendefrequenz des Lesegeräts herstellen, wenn also die Sendefrequenz mit der Eigenfrequenz des Objekts übereinstimmt. Bei der Eigenfrequenz eines Systems schwingt dieses nach einmaliger Anregung weiter, solange es seine Dämpfung erlaubt. Über eine Steuerung des reflektierten Signals werden die Daten ähnlich wie bei der induktiven Kopplung an das Lesegerät übermittelt.

2.6. Frequenzbereiche und Reichweiten

Für Energie und Datenübertragung werden abhängig von den Funktionsprinzipien Felder oder Wellen in unterschiedlichen Bereichen des Radio– und Mikrowellen–Frequenzbandes genutzt.

RFID-Systeme für die Produktidentifizierung arbeiten meist im Langwellenbereich zwischen 100 kHz und 135 kHz oder im Kurzwellenbereich bei 13,56 MHz. Komplexere Systeme mit höheren Reichweiten arbeiten auch im Mobilfunkbereich um 900 MHz, in Nordamerika auf 915 MHz, in Europa auf 868 MHz. Auch das Mikrowellenspektrum ist mit den Frequenzen 2,45 GHz und 5,80 GHz für RFID-Systeme erschlossen. Die unterschiedlichen Frequenzbereiche, die für die Energie– und Datenübertragung genutzt werden können, weisen je nach Anwendungsgebiet Vor- und Nachteile auf. Je höher die Frequenz, desto mehr Daten können pro Zeiteinheit übertragen werden. Ist es für eine Anwendung wichtig, viele Daten in kurzer Zeit zu lesen, so würde sich eine hohe Kommunikationsfrequenz anbieten.

Flüssigkeiten oder Feuchtigkeit können bei hohen Frequenzen aber zu Problemen führen, da sie die Feld– oder Wellenausbreitung erschweren. Bei niedrigen Frequenzen führen metallische Objekte zu Störungen (wenn sich beispielsweise ein RFID-Tag auf einer Blechdose befindet). Mit Sendefrequenzen im Langwellenbereich (unterhalb 135 kHz) werden heute in der Regel Übertragungsweiten von ca. 1,5 Meter erreicht. Bei 13,56 MHz liegen diese noch bei knapp einem Meter. Bei Systemen im Mobilfunk– und Mikrowellenbereich können heute auch schon auch 3 bis 7 Meter Reichweite überbrückt werden. Die effektive Reichweite hängt von den Umgebungsvariablen ab: Störeffekte wie Flüssigkeiten oder Metallteile, die bei den verschiedenen Frequenzen unterschiedlich wirken, verringern die Reichweite.

Eindeutige Grenzen für die maximal erzielbare Reichweite, die ein wichtiges Kriterium nicht nur für den Einsatz sondern auch für unerwünschte Nebeneffekte sind, können grundsätzlich nicht genannt werden. Abgesehen von den oben genannten Beeinträchtigungen der Feld– oder Wellenausbreitung hängt die überbrückbare Entfernung entscheidend von der Sendeenergie und der Empfangsempfindlichkeit der Übertragungsstrecke sowie von der Störungsempfindlichkeit der Signalcodierung ab. Standardisierungsorganisationen und Gesetzgeber beschränken heute lediglich die Sendeleistung von RFID-Lesegeräten.

Dahinter stehen Überlegungen zum Gesundheitsschutz von Menschen. In Europa gelten u.a. die europäischen Normen 50357 und 50364, zur »Begrenzung der Exposition von Personen gegenüber elektromagnetischen Feldern von Geräten, die im Frequenzbereich von 0 Hz bis 10 GHz betrieben und in der elektronischen Artikelüberwachung (EAS), Hochfrequenz-Identifizierung (RFID) und ähnlichen Anwendungen verwendet werden«.

Dass damit gleichzeitig die Maximalreichweite begrenzt wird, kann daraus keinesfalls abgeleitet werden. Sie ist abhängig von der Technologie der Empfangskomponenten und der Komplexität der Signalaufbereitung. In wenigen Jahren können Grenzen um Größenordnungen übersprungen werden, die aus der Sicht des gegenwärtigen Standes von Methodik und Technologie postuliert werden. Das zeigen Beispiele wie etwa die Entwicklung des Ethernet (10 MHz schienen anfangs die Obergrenze zu sein), die Steigerung der Datenraten über Telefonleitungen oder die Ausweitung der Kanalkapazität von Satellitenfunkstrecken bei immer kleineren Parabolantennen.

Forschung und Entwicklung tragen mit Sicherheit weiterhin dazu bei, dass die bisherigen RFID-Konzepte ausgebaut und optimiert werden und sich damit auch weitere neue Anwendungsfelder erschließen. Der Polymer-Technik kommt dabei eine Schlüsselrolle zu. Mit ihrer Hilfe sollen Tags nur noch aus organischen Polymerstrukturen bestehen. Sollten einmal Chips auf Silizium-Basis und Antennen aus Metall entfallen, würde dies entscheidend zur Umweltverträglichkeit der RFID-Tags beitragen — ein nicht zu vernachlässigender Aspekt, wenn man an die weite Verbreitung, die hohen Stückzahlen und das zukünftige Potenzial denkt. Ein primäres Ziel der Weiterentwicklung ist es, die Produktion preisgünstiger zu machen und dadurch der Masseneinführung zu einem Schub zu verhelfen. Wenn zukünftige Tags sich noch einfacher in bestehende Produktverpackungen integrieren lassen, ist es lediglich eine Frage der Zeit, bis RFID für die Logistik im großen Stil eingesetzt wird.

In den Diskussionen über das RFID-Thema muss auch über missbräuchliche Verwendung und über die Notwendigkeit von Sicherheitsmaßnahmen gesprochen werden. Wo Daten, die mittels Funk gelesen werden können, nur unzureichend geschütztsind, da gewinnt der Aspekt der Lesereichweite an Bedeutung und damit die Frage, wie die Datenabfrage kontrolliert werden kann. Mit leistungsstarken Prozessoren können komplexe Authentifizierungs- und Verschlüsselungsverfahren realisiert werden, es können aber auch vielfältige Daten gesammelt werden, mit denen umfangreiche Bewegungsprotokolle etc. erstellt werden können.

Ob dem Einsatz solcher komplexeren und leistungsfähigeren Systeme Kostengründe entgegenstehen, ist lediglich eine Frage der Nachfrage und einer durch Produktionsmengen gesteuerten Preisentwicklung. Die Objektidentifikation ist einerseits ein wichtiger Bestandteil vieler Prozesse in der Produktion und Logistik. Durch ihre Automatisierung können Unternehmen ihre bestehenden Abläufe optimieren und langfristig kontrollieren.

Die Vorteile der RFID-Technik in der Industrie bringen andererseits auch Gefahren für die Verbraucher mit sich. Sie treten spätestens dort auf, wo individuell gekennzeichnete Produkte über die Ladentheke wandern. Wenn Objekte jederzeit automatisch erkannt werden können, dann ist der Personenbezug ebenso leicht möglich. Und hier schafft RFID ein spezielles Problem: Menschen identifizieren sich in der Regel wissentlich, zum Beispiel bei einer förmlichen Vorstellung „Guten Tag, mein Name ist ...“, oder man wird zur Identifizierung mittels Personalausweis, Reisepass oder Kundenkarte aufgefordert. RFID macht es jedoch möglich, dass Menschen auch ohne ihr Wissen und sogar gegen ihren Willen erkannt werden können: Gefährdet wird die Anonymität im Alltag. Dies ist eine neue Dimension der Bedrohung der Privatsphäre.

Bei den Verantwortlichen für Entwicklung und Anwendung muss ein Bewusstsein dafür geschaffen werden, dass RFID nicht per se nur Vorteile bringt. Es liegt (auch) in ihren Händen, dass die Systemrisiken bereits in den frühen Konzept und – Entwurfsstadien erkannt und minimiert werden. Darüber hinaus ist der Gesetzgeber in die Pflicht genommen, vorausschauend im Interesse der Bürger zu handeln. Im Moment läuft er im Rennen um die Verbraucherinteressen mit der Wirtschaft allerdings nur mäßig motiviert hinterher ...

Frequenzbereiche				
Parameter	Niedrigfrequenz	Hochfrequenz	Ultrahochfrequenz	Mikrowelle
Frequenz	125 – 134 kHz	13,56 MHz	868 bzw. 915 MHz	2,45 bzw. 5,8 GHz
Leseabstand	bis 1,2m	bis 1,2m	bis 4m	bis zu 15m (in Einzelfällen bis zu 1km)
Lesegeschwindigkeit	langsam	je nach ISO-Standard*	schnell	sehr schnell (aktive Transponder)
Feuchtigkeit**	kein Einfluss	kein Einfluss	negativer Einfluss	negativer Einfluss
Metall**	negativer Einfluss	negativer Einfluss	kein Einfluss	kein Einfluss
Ausrichtung des Transponders beim Auslesen	nicht nötig	nicht nötig	teilweise nötig	teilweise nötig
Weltweit akzeptierte Frequenz	ja	ja	EU 868 MHz USA 915 MHz	teilweise (nicht EU)
Heutige ISO-Standards	11784/85 und 14223	14443, 15693 und 18000	14443, 15693 und 18000	18000
Typische Transponder-Bautypen	Glasröhrchen-Transponder, Transponder im Plastikgehäuse, Chipkarten Smart Label, Chipkarten	Smart Label, Industrie-Transponder, weltweit anerkannter Standard für Einzelprodukte für passive Transponder	Smart Label, Industrie-Transponder	Großformatige Transponder
Beispielhafte Anwendungen	Zutritts- und Routenkontrolle, Wegfahrsperren, Wäschereinigung, Gasablesung, Chippen von Tieren oder Menschen	Wäschereinigung, Asset Management, Ticketing, Tracking & Tracing, Pulk-Erfassung (Einzelprodukte)	Palettenerfassung, Container-Tracking	Straßenmaut, GPS, Container-Tracking

* unter 1 s bis 5 s bei ISO 14443 (5 s für 32 kByte), im Mittel 0,5 m/s Vorbeibewegung bei ISO 15693

** Der Einfluss von Metall und Flüssigkeiten variiert je nach Produkt. Auch werden mittlerweile RFID-Tags angeboten, die den Einsatz (nach Herstellerangaben) auch im Niedrigfrequenzbereich erlauben; beispielsweise „(rfid)-onMetal-Label" von Schreiner Logidata

Quelle: BSI – Bundesamt für Sicherheit in der Informationstechnik (BRD)

3. RFID-ANWENDUNGEN HEUTE

In vielen Bereichen hat die RFID-Technik bereits Einzug gehalten und ist dabei auch weitere, zukunftsorientierte Anwendungsfelder zu erschließen:

- **Logistik/Supply Chain (Warenidentifikation und Verfolgung, Fluggepäckverfolgung, Paketdienste)**
- **Prozesskontrolle/Produktion (Werkzeugkontrolle, Produktionsverfolgung/ Fertigungshistory, Merkmal für Fälschungssicherheit (Pharmaindustrie))**
- **Sicherheits- und Zahlungssysteme (Zugangssysteme, Diebstahlreduktion, Ticketing, elektronische Bezahlung, Wegfahrsperre, Smart-Pass)**

- **Tieridentifikation (Landwirtschaft, Brieftauben, Populationsverfolgung von Insekten)**
- **Archivierungssysteme (Akten- und Dokumentenerfassung, Bibliotheken, Inventarisierung)**
- **weitere Anwendungen in Medizin/Chemie, für Menschen mit Aktivitätsbeschränkung, Gasbehälter (zur Füllstandskontrolle), Sportveranstaltungen, Implantate usw.**
- **militärische Anwendungen**

3.1. Anlagenverwaltung/Facility Management

Klimaanlagen oder Entlüftungsschächte, die regelmäßig zu warten sind, können RFID-Chips erhalten. Diese dokumentieren die regelmäßige Wartung und möglicherweise an der Anlage durchgeführte Reparaturen. Nebenbei ermöglicht das System auch eine lückenlose Kontrolle der Arbeit des Wartungspersonals.

Die Fraport AG, Eigentümerin des Flughafens Frankfurt, betreut im Rahmen des Immobilien- und Facility-Managements rund 420 Gebäude und Anlagen. Eine zentrale Aufgabe ist die regelmäßige Instandhaltung und Kontrolle von technischen Komponenten mit gesetzlich vorgeschriebener Wartung. Die Fraport AG nutzt RFID-Chips in Verbindung mit der Software Mobile Asset Management (mobile Anlagenverwaltung) von SAP, um Lüftungssysteme zu überwachen und zu warten. Mobile Endgeräte des Wartungspersonals speichern die täglichen Aufträge und erfassen die RFID-Tags an den Lüftungssystemen. Anschließend übermitteln sie die Ergebnisse der Wartungsarbeiten an das ERP-System.

Die RFID-Chips gewährleisten in diesem Fall, dass jeder Abschnitt der Anlagen überprüft wird. Die per Funk übertragenen Daten bestätigen den Wartungsvorgang.

3.2. Fertigung in der Industrie

Vor allem die traditionell unter besonderem Kostendruck stehende Automobilindustrie hat in den letzten Jahrzehnten viele Produktionsschritte automatisiert, wie andere Unternehmen mit Massenfertigung auch. Allerdings müssen die Firmen heute in der Lage sein, maßgeschneiderte Produktvarianten herzustellen, um die gestiegenen Ansprüche der Verbraucher zu befriedigen – auch hier ist die Automobilindustrie Vorreiter.

Viele Varianten eines Produkts werden auf derselben Fertigungslinie erstellt, was eine eindeutige Identifikation des zu bearbeitenden Objekts an jeder Fertigungsstation notwendig macht. Ein Steuerungssystem für die einzelnen Fertigungsstationen sorgt dann dafür, dass nur die diesem Objekt zugeordneten Schritte ausgeführt werden (im Falle der Automobilindustrie vielleicht eine Lackierung dieses speziellen Autos in Silbergrau).

RFID-Systeme reduzieren nicht nur die Kosten an den einzelnen Fertigungsstationen, sie haben viele weitere Vorteile gegenüber anderen Automatisierungskonzepten. So sind RFID-Systeme - im Gegensatz beispielsweise zu Barcodes - weitgehend unempfindlich gegenüber rauen Umgebungsbedingungen wie Schmutz, Staub oder Licht.

3.3. Elektronische Wegfahrsperre

Nicht nur die Zutrittskontrolle kann über RFID-Technologie erfolgen.

Wegfahrsperren wurden Mitte der 1990er Jahre in Deutschland in großem Stil eingeführt, um die in den 90er Jahren sprunghaft angestiegenen Kfz-Diebstähle einzudämmen. RFID-Chips, zum Beispiel im Schlüssel, können als elektronische Wegfahrsperre dienen, so dass ein Wagen nicht ohne den dazugehörigen Schlüssel zu starten ist. Um das Kurzschließen des Zündschlosses (eine der verbreitetsten Diebstahlsmethoden) unmöglich zu machen, wird bei jedem Start des Motors die Echtheit des Zündschlüssels elektronisch geprüft. Dazu muss die Kommunikation zwischen Lesegerät im Fahrzeug und Tag im Autoschlüssel verschlüsselt werden.

Möglich ist es auch, mittels eines eingebauten Chips das Rad eines Einkaufswagens zu blockieren, sobald es über eine festgelegte Grenze rollt. Zum Einsatz kommen ausschließlich induktive Systeme, da hier keine Stützbatterie benötigt wird und die Systeme somit vollständig wartungsfrei sind.

3.4. Öffentlicher Personennahverkehr

In den kommenden Jahren lässt die Verwendung von RFID-Technik im öffentlichen Personennahverkehr große Zuwächse erwarten. Bis heute sind der klassische Fahrscheinverkauf und die zumindest stichpunktartigen Kontrollen der Fahrgäste mit hohen Kosten verbunden. RFID-Tags stellen eine billigere und zuverlässigere elektronische Variante dar, sie sind witterungsbeständig, langlebig und komfortabel (zB Abbuchung von der Karte, ohne sie aus dem Geldbeutel zu nehmen). Bei Pre-paid-Systemen wird die Karte mit einem Geldbetrag geladen und vor oder nach jeder Fahrt ein entsprechender Betrag abgebucht, vergleichbar mit den Mensa-, bzw. Kantinenkarten vieler Universitäten oder Firmen (ein weiteres Beispiel für RFID-Anwendungen). Im Falle eines Abo-Systems würde bei der Einlasskontrolle überprüft, ob der Fahrgast im Besitz einer gültigen Karte ist, die wochen-, monats- oder jahresweise, aber auch in einem frei definierbaren Zeitraum gültig sein könnte. Beide Systemvarianten sind nebeneinander möglich.

Bahncard und Fahrkarten

Beim Einsatz von RFID in Fahrkarten liegt die Erstellung von Bewegungsprofilen auf der Hand: Wenn jede Fahrt einzeln abgerechnet wird, sind Strecke und Zeitpunkt automatisch abgespeichert. Anonymes Reisen ist dann Vergangenheit. Die Deutsche Bundesbahn hat gleich direkt ihre »Dauerausweise« mit RFID versehen…

Die »Bahncard 100« enthält seit April 2005 einen RFID-Chip. Die BC100 ist die Luxus-Variante der Bahncard, mit der Bahnfahren für ein Jahr kostenlos ist. Auch viele andere öffentliche Verkehrsmittel oder Carsharing-Angebote der Bahn können damit genutzt werden. Nicht tolerierbar ist, dass die Bahn diesen Chip in der Karte quasi ohne Information an ihre Kunden eingesetzt hat - bis heute weiß kaum jemand, dass die BC100 verwanzt ist.

Außerdem gibt es keine Wahlmöglichkeit, sich auch eine Bahncard ohne Chip ausstellen zu lassen - während es z.B. bei anderen Bahncards möglich ist, auf Wunsch kein Foto aufdrucken zu lassen. Immerhin: Durch das 100%-Rabatt-Prinzip bei der BC100 mit RFID-Chip werden die Fahrten nicht automatisch erfasst, denn man löst ja kein Ticket mehr. Wenn aber RFID-Lesegeräte an den Bahnsteigen aufgestellt werden, ist das auch nicht mehr nötig, dann erfassen diese Antennen die BC100-Kunden automatisch und unbemerkt und das Bewegungsprofil ist perfekt. Ein Paradies für Überwachungs-Trolle: Ausreichend Videoüberwachung für eine schnelle Identifizierung gibt es ja auf Bahnhöfen sowieso schon.

Der Verkehrsverbund Rhein-Ruhr (VRR) setzt RFID seit Februar 2004 in seinen Dauer-Fahrkarten in Form von Chipkarten ein, wie der verbundeigenen Homepage zu entnehmen ist. Auf den Chips befinden sich Daten zur Fahrtberechtigung (Daten zur räumlichen und zeitlichen Gültigkeit), Name und Geburtsdatum des Benutzers. Der VRR gibt außerdem auf seiner homepage indirekt zu, dass ein Auslesen der Chips möglich sei.

Sonst würde wohl nicht gesondert auf Schutzmöglichkeiten (Abschirmung mittels eines Metallbehälters) hingewiesen werden.

Dies ist nicht sehr vertrauenserweckend für den RFID-Einsatz in diesem Bereich. Es unterstützt vielmehr die Vorbehalte gegen die Verwendung der RFID-Technik in bestimmten Bereichen. Eine abschließende Anekdote zu den sogenannten Schokotickets verdeutlicht die möglichen Risiken des Auslesens der Schnüffelchips, wenn auch hier auf eine mehr oder weniger komische Art und Weise: Gerüchteweise sollen von einem Einzelhandelsgeschäft an einer Bushaltestelle im Gebiet des VRR rätselhafte Schrott-Daten erfasst worden sein - bis sich heraus stellte, dass die Tore des Ladens die »Schoko-Tickets« der Schülerinnen und Schüler erfasste, die an der Bushaltestelle vor der Tür warteten. Jedoch konnten wir bislang die Quelle oder Stichhaltigkeit dieses Gerüchtes noch nicht ausfindig machen. Quelle: http://www.foebud.org

3.5. Tierhaltung

Neben der Identifikation von Waren, Behältern und Menschen, ermöglicht RFID auch die Identifikation von Tieren. In Nutztiere lassen sich beispielsweise Glastransponder injizieren, auf denen sich neben Daten zur Identifizierung auch Informationen über Fütterung und Medikamentengaben speichern lassen. In der Tierhaltung werden RFIDs schon seit längerem angewendet. So werden in High-Tech-Kuhställen automatisierte Fütterungsanlagen eingesetzt, bei denen der Fütterungsautomat für jedes Tier genau die vorgesehene Futtermenge ausgibt.

Hat eine Kuh die vorgesehene Tagesration bereits gefressen, gibt der Fütterungsautomat einfach kein weiteres Futter aus. Umgekehrt lässt sich überwachen, ob eine Kuh zu wenig oder gar nicht frisst. Eine automatisierte Milchmengen-Statistik lässt sich in die Melkanlage integrieren. In den letzten Jahren gibt es Bestrebungen in der Landwirtschaft, die RFID-Technologie auch zur betriebsübergreifenden Kennzeichnung der Tiere für die Seuchen- und Qualitätskontrolle sowie zur Herkunftsverfolgung einzusetzen.

RFID-Technik wird auch zur Haustieridentifizierung eingesetzt. Der Tierpass registriert alle durchgeführten Impfungen, und sollte ein Haustier verloren gehen, ist eine RFID-Erkennung sehr sinnvoll, da über die Registrierungsnummer der Besitzer schnell ermittelt werden kann. Darüber hinaus gibt es weitere Anwendungsmöglichkeiten, beispielsweise spezielle Katzen- oder Hundetüren, die nur die eigene Katze oder den eigenen Hund ins Haus lassen. Eine automatische Fütterungsanlage ist auch für Kleintiere denkbar. Tags zur Tierkennzeichnung haben teilweise nur die Größe eines Reiskorns und werden den Tieren mit einer Spritze unter die Haut injiziert.

3.6. RFID-Implantate

Ähnliche RFID-Tags in Form von kleinen Glaskapseln finden seit kurzem auch beim Menschen Anwendung. Die Tags können mittels einer Spritze unter örtlicher Betäubung innerhalb weniger Minuten unter die Haut implantiert werden. Sichere Zugangssysteme zu Computern oder Gebäuden sind bereits im Einsatz.

Das Implantieren eines RFID-Chips allein zur Bezahlung in einer einzigen Bar, halten wohl die meisten für unakzeptabel und die angepriesene bequeme Zahlweise per Rechnung, die nach Hause kommt, ist fadenscheinig, angesichts der bereits vorhandenen Möglichkeiten per Kreditkarte zu bezahlen. Egal wie modern der Chip im Oberarm ist, er ist zudem ein Fremdkörper, der per Injektion unter die Haut gespritzt wird. Wem könnte der Chip also dienen?

Der/dem Clubbetreiber/-in zur Kundenbindung und als Sicherheit für die Bezahlung, da ihr/ihm die/der Kundin/Kunde nicht nur namentlich, sondern auch mit Adresse bekannt ist. Bei näherem Betrachten erweist sich die Idee mit dem Chip im Arm eher als Flop. Je mehr Chips im Oberarm, desto wahrscheinlicher ist zudem, dass diese sich untereinander beim Lese-/ Schreibvorgang stören. Offen ist, wie die/der Kundin/Kunde kontrollieren kann, ob das auf den Chip gebuchte Ge- tränk auch wirklich von ihr/ihm konsumiert wurde.

Andere RFID-Anwendungen scheinen auf den ersten Blick nützlich. Sie sparen Kosten, Zeit und Arbeitskräfte, indem sie Handelswege, Kassiervorgänge, logistische Schritte und Bestellungen etc. automatisieren. Doch gibt es auch hier eine Kehrseite der Medaille, wenn Arbeitsplätze verschwinden und menschliche Serviceleistungen einem Automaten weichen. Aber auch in der Medizin eröffnen RFID-Implantate ein breites Anwendungsgebiet:

Sie können zur Identifikation von Patienten dienen und so deren Verwechslung im Krankenhaus oder einer falschen Medikation (Art, Dosis, Zeit) vorbeugen. Von besondern Vorteil sind sie bei Patienten, die sich nicht verständlich machen können, wie Bewusstlosen oder Alzheimer-Kranken. Der Chip muss nicht implantiert werden, die beschriebene Funktionalität lässt sich auch durch einen Chip in Form eines Armbandes gewährleisten. Bei einer abnehmbaren Identifikationsquelle ist die Fehlermöglichkeit aber höher.

3.7. RFID-Sensoren

Neben der reinen Identifikation können heutige Tags auch mit Sensoren verknüpft werden und somit einen ganz neuen Anwendungsbereich eröffnen. Sie werden hauptsächlich dort genutzt, wo man keine kabelgebundenen Sensoren einsetzen will oder kann. Dabei ist der entscheidende Vorteil von RFIDs im Vergleich zu anderen Funkübertragungsstandards wie Bluetooth oder DECT, dass der Sensor über das Feld der Datenkommunikation gleichzeitig seine Energie erhält, die Tags mit integrierten Sensoren also rein passiv sind. Bei industriellen Anwendungen an beweglichen Teilen entfallen so die fehleranfälligen mechanischen Schleifkontakte. So lässt sich der Reifenfülldruck von Fahrzeugen messen oder die Temperatur ätzender Flüssigkeiten in der chemischen Industrie durch säurebeständige (glasgekapselte) RFID-Sensoren ermitteln.

Im Bereich der Logistik stattet man bereits Container mit Sensoren in RFID-Technik aus, um sensible Güter auf ihrem Weg zum Bestimmungsort zu überwachen. Die Messwerte wie Temperatur, Feuchtigkeit oder Erschütterungen werden meist im Tag zur späteren Auswertung gespeichert, um später beispielsweise die Einhaltung der Kühlkette bei Lebensmitteltransporten nachweisen zu können.

3.8. e-Pass - Elektronischer Reisepass mit biometrischen Daten

Seit 1997 befasste sich die ICAO, eine Unterorganisation der Vereinten Nationen, mit der Einführung von elektronisch auswertbaren biometrischen Merkmalen in Reisedokumenten. Im Jahre 2003 führte dies zur Vorstellung einer unter der Bezeichnung „Blueprint" (engl. für „Blaupause") bekannt gewordenen Empfehlung. Sie hält die UN-Mitgliedsstaaten dazu an, zukünftig biometrische Merkmale der Inhaber elektronisch auf dem Reisedokument zu speichern. Die Kriterien für die Auswahl der zu verwendenden Techniken sind weltweite Interoperabilität, Einheitlichkeit, technische Zuverlässigkeit, Praktikabilität und Haltbarkeit. Die vier zentralen Punkte des „Blueprint" sind die Verwendung von kontaktlosen Chips (RFID), die digitale Speicherung des Lichtbilds auf diesen Chips, wobei weitere Merkmale wie Fingerabdrücke oder Irismuster ergänzt werden können, die Verwendung einer definierten logischen Datenstruktur (Logical Data Structure, LDS) und ein Verfahren zur Verwaltung von digitalen Zugangsschlüsseln (Public Key Infrastructure, PKI). Die Vorgaben wurden in der Weiterentwicklung des Standards 9303 der ICAO zusammengefasst.

Am 13. Dezember 2004 beschloss der Rat der Europäischen Union auf Druck der USA, die Pässe der Mitgliedsstaaten gemäß diesem Standard mit maschinenlesbaren biometrischen Daten des Inhabers auszustatten. Die Einführung des neuen Reisepasses wurde von den EU-Staaten vereinbart. Neben Österreich haben auch Belgien, Schweden, Großbritannien, Deutschland und Frankreich mit der Umstellung bereits begonnen. Seit Mitte Juni 2006 gibt es auch in Österreich den RFID-Reisepass mit Seit dem 16. Juni 2006 werden in Österreich biometrische Pässe (sogenannte „Sicherheitspässe") ausgegeben, die mit einem kontaktlosen Chip versehen sind. Einem integriertem Chip, auf dem persönliche Daten und Foto gespeichert werden. Hierfür wird ein Passbild benötigt, das bestimmte Kriterien an die biometrische Erfassung erfüllen muss. Und er ist nicht billig für die Bürger/-innen.

Das Argument der „inneren Sicherheit" ist umstritten. Es wird argumentiert, dass der österreichische oder deutsche Reisepass schon vor der Biometrisierung als eines der fälschungssichersten Dokumente weltweit gegolten hat. Es sei beispielsweise kein Terrorakt in Europa bekannt, zu dessen Durchführung ein gefälschter Pass oder Personalausweis benutzt wurde. Dem wird entgegen gehalten, dass bereits die RAF-Terroristen regelmäßig falsche oder verfälschte Dokumente missbrauchten. Der neue Reisepass mit biometrischen Verfahren ist heftig umstritten. Die biometrischen Daten werden digital kodiert auf einem RFID-Chip gespeichert, der sich in einem RFID-Inlay in der Passbuchdecke befindet. So soll es schwieriger werden, den Ausweis zu fälschen, und einfacher, bei Grenzkontrollen die Identität festzustellen. Durch die neue Technologie erhöhen sich natürlich die Kosten der BürgerInnen für den Reisepass.

Anwendungen

Mit der Einführung von e-Pässen ist es möglich die Kontrollprozesse beim Grenzübertritt teilweise oder vollständig zu automatisieren. Durch geeignete Verfahren und Kombination von Personenvereinzelung, Dokumentenechtheitsprüfung und biometrischer Inhaberverifikation können Reisende in Selbstbedienung entsprechend ausgestattete Kontrollpunkte bedienen. Insbesondere Flughafenbetreiber und Grenzschutzbehörden erwarten eine Entlastung des Kontrollpersonals und eine Verringerung der Wartezeiten für Passagiere. Im Juni 2007 hat erstmalig in Europa der Internationale Flughafen von Faro in Portugal mehrere derartige mit biometrischer Gesichtserkennung ausgestattete Gates in Betrieb genommen.

Elektronische Sicherheitsmerkmale

Die ICAO spezifiziert einige Sicherheitsmechanismen, die verschiedenen Zwecken dienen, wovon aber nur die Passive Authentication verpflichtend zu implementieren ist. Die EU weicht von den ICAO-Vorgaben ab und definiert weitere dieser Sicherheitsmechanismen als verpflichtend. Neben der Passive Authentication sind das die Basic Access Control sowie die Extended Access Control für Fingerabdrücke.

Passive Authentication (verpflichtend)

Die Passive Authentication dient der Sicherstellung der Authentizität der elektronisch gespeicherten Daten, indem diese mit einer elektronischen Signatur gesichert werden. Dadurch wird jede nachträgliche Modifikation der Daten vom Lesegerät detektiert, da dabei die Signatur ungültig wird. Die Erstellung einer 1:1-Kopie wird jedoch ausdrücklich nicht verhindert.

Basic Access Control (optional)

Basic Access Control ist ein Mechanismus zur Wahrung der Privatsphäre, bei dem das elektronische Lesen der Daten erst freigegeben wird, wenn das Lesegerät nachgewiesen hat, dass es Kenntnis vom Inhalt der optisch auszulesenden maschinenlesbaren Zone hat. Dadurch wird sichergestellt, dass der Passinhaber das Dokument physisch demjenigen, der es auslesen will, übergeben hat oder wenigstens geöffnet gegen einen optischen Scanner hält, was als Einverständnis zum elektronischen Lesen gewertet wird.

Active Authentication (optional)

Unter Active Authentication versteht man einen Mechanismus zum Verhindern von 1:1-Kopien. Dabei kommt ein asymmetrisches Kryptosystem zum Einsatz: Der öffentliche Schlüssel befindet sich in den signierten Daten deren Authentizität von der Passive Authentication sichergestellt wird, während der private Schlüssel im gesicherten Speicher des Chips ist und nicht ausgelesen werden kann. Der Chip kann dann dem Lesegerät seine Kenntnis des privaten Schlüssels über ein Challenge-Response-Verfahren nachweisen. Dabei generiert das Lesegerät eine Zufallszahl, schickt diese zum Chip, wo sie signiert und die Signatur zurückgeschickt wird. Wenn die Signatur stimmt, ist hinreichend sichergestellt, dass der Chip im Besitz des privaten Schlüssel ist und daher nicht kopiert wurde.

Eine mögliche Schwachstelle dieses Verfahrens ergibt sich, wenn das Lesegerät der Zufallszahl eine versteckte Semantik zuordnet. Ein Inspektionssystem könnte beispielsweise Ort und Zeit in die Zufallszahl kodieren, die dann vom Chip signiert wird, und die Signatur aufbewahren. Damit könnte dann zu einem späteren Zeitpunkt eine dritte Partei davon überzeugt werden, dass sich der Chip -und damit der Pass und dessen Inhaber- zu einem bestimmten Zeitpunkt an einem bestimmten Ort befunden haben.

Extended Access Control (optional)

Die Extended Access Control ist ein Mechanismus zur Verwaltung von Zugriffsrechten. Während die Daten die mit Basic Access Control gelesen werden können – also Name, Geburtsdatum, Gesichtsbild, etc. – ohnehin jedermann zugänglich sind, der im physischen Besitz des Passes ist, ist für die Zukunft die Aufnahme zusätzlicher, sensiblerer Daten geplant, z. B. der Fingerabdrücke. Über Extended Access Control sollen dann diese zusätzlichen Daten geschützt werden, wobei die Kontrolle darüber, welche Staaten welche der zusätzlichen Daten lesen können, bei den passausgebenden Staaten liegen soll.

Die genaueren Details werden von ICAO nicht spezifiziert und obliegen den passausgebenden Staaten.Die Spezifikation bildet die Grundlage für den EU-Ratsbeschluss vom 28. Juni 2006.

Gechippter Reisepass

Die Reisepässe enthalten einen integrierten RFID-Chip im oberen Umschlagsdeckel, auf welchem neben den bisherigen Passdaten auch ein digitales Foto gespeichert ist. Auch die digitalisierten Merkmale Fingerabdrücken können darauf gespeichert sein. Um auf die auf dem Chip gespeicherten Daten zugreifen zu können, ist ein Schlüssel notwendig, der sich in der maschinenlesbaren Zone (MRZ) des Ausweises befindet. Da diese Zone nur optisch lesbar ist, ist damit ein direkter Zugriff auf den Pass erforderlich, der direkt an das Lesegerät gehalten oder aufgelegt werden muss.

Das Auslesen eines sich in einer Jackentasche befindenden Reisepasses ist also nicht möglich, da Sichtkontakt vorhanden sein muss. Das Konzept ist auch auf andere Ausweise anwendbar, zum Beispiel auf Personal-, Mitarbeiter- oder Kundenausweise. Hier gilt es zu verhindern, dass unberechtigte Dritte Kenntnis von den auf den Chips gespeicherten personenbezogenen Daten erlangen. Es ist also darauf zu achten, dass Chips zum Einsatz kommen, die nur im Zentimeterbereich ausgelesen werden können.

Das hat zwar den Nachteil, dass Beschäftigte oder Kundinnen/Kunden den Ausweis direkt an das Lesegerät halten müssen, bietet aber den Vorteil, dass die Daten weder mit einem Lesegerät aus größerer Entfernung noch aus unmittelbarer Nähe unbemerkt und unberechtigt lesbar sind. Außerdem besteht die Option, Schlüssel und Chip getrennt zu halten, um auf diese Weise ein unbefugtes Auslesen zu verhindern.

Das RFID-Inlay des deutschen Reisepasses besteht z.B. aus einer Antennenspule und dem RFID-Chip, der von der Bundesdruckerei bei den Herstellern Philips (Typ SmartMX) oder Infineon (Typ 66CXLxxxP) bezogen wird und mit 72kB bzw. 64kB EEPROM zur Speicherung der biometrischen Daten ausgestattet ist. Die Chips haben einen kryptographischen Koprozessor, über den die Kommunikation zwischen Ausweis und Lesegerät verschlüsselt wird. In der Ausbaustufe 1 enthält der e-Pass, der seit kurzem erhältlich ist, im RFID-Chip nur die personenbezogenen Daten und als einziges biometrisches Merkmal das Gesichtsbild, das im JPEG-Bildformat kodiert etwa 15kB des EEPROM-Speichers belegt. In der Ausbaustufe 2, die 2007 startete, wird zusätzlich ein Fingerabdruck als biometrisches Merkmal mit aufgenommen werden. Jedes Lesegerät muss durch das den Ausweis ausstellende Land zertifiziert werden. Dieses kann so bestimmen, welches Land welche Informationen aus dem Datenbereich des RFID-Chips auslesen darf.

Britische RFID-Pässe bereits »gecrackt«

Seit März 2006 gibt auch die britische Regierung neue Reisepässe aus. Dabei werden persönliche Daten und Foto auf einem RFID-Chip gespeichert. Mehrere Millionen der neuen Pässe befinden sich in Großbritannien bereits im Umlauf. Einem Sicherheitsexperten ist es gelungen, in weniger als 48 Stunden Daten aus den neuen britischen RFID-Chip-Reisepässen auszulesen. Auch das Klonen eines Chips sei kein Problem, sagen Spezialisten. Das britische Innenministerium spielt das Problem herunter.

Dem britischen Sicherheitsexperten Adam Laurie ist es vor kurzem gelungen, Daten aus den Hochsicherheitspässen auszulesen. Mit einem RFID-Lesegerät, das er um rund 250 Pfund kaufte, machte sich Laurie daran, Verbindung mit dem in einem neuen Pass eingeschweißten Chip aufzunehmen. Der Zugang habe sich als erstaunlich einfach herausgestellt, zeigte sich Laurie gegenüber der britischen Zeitung »theGuardian« überrascht.

Zwar komme zur Verschlüsselung der Unterhaltung zwischen Chip und Lesegerät der Standard 3DES zum Einsatz, der die dreifache Sicherheit eines militärischen Verschlüsselungsstandards biete, der Key zur Verschlüsselung setze sich jedoch aus Passnummer, Geburtsdatum des Eigentümers und Verfallsdatum des Passes zusammen, sagte Laurie. Das sei in etwa so, als würde man ein Haus mit einer Stahltür schützen, den Schlüssel dazu aber unter die Fußmatte vor der Tür legen, gab der Sicherheitsexperte zu bedenken. Innerhalb von 48 Stunden konnte Laurie die Verschlüsselung knacken und die Daten aus dem Chip im Pass auslesen.

Deutsche Reisepässe »geklont«

Indem Daten ausgelesen werden können, sei es auch kein Problem, den Pass zu klonen - also die Daten auf einen anderen Chip zu duplizieren -, meinen hingegen Sicherheitsexperten.

Wie das funktioniert, hat der deutsche Techniker Lukas Grunwald an Hand der deutschen RFID-Reisepässe vorgeführt. Auf den Blackhat Briefings, der Fachmesse für Sicherheitsexperten in Las Vegas, demonstrierte Grunwald eine Methode, wie die Funkchips in den neuen deutschen Biometrie-Pässen auszulesen und die Chips dann zu klonen sind.

Bei den österreichischen Chip-Pässen soll das Klonen der Daten durch ein zusätzliches Prüfverfahren verhindert werden. Die österreichischen Passbehörden sind mit dem ePassport Verification System des US-Herstellers 3M ausgestattet. Mit diesem Gerät soll sich der Bürger auf dem Amt alle Daten auf dem RFID-Chip seines Passes anzeigen lassen können. Fast alle.

Ein dem Pass beigelegter Chip mit falschen (weil geklonten) Daten könnte so ein RFID-Lesegerät täuschen. Jeder Gegencheck eines Zollbeamten im analogen Pass brächte jedoch die Manipulationen ans Tageslicht.

Biometrische Daten verschärfen das Problem weiter. Das Problem könnte sich noch weiter verschärfen, sobald auch biometrische Daten wie etwa Fingerabdrücke auf den Chips gespeichert werden. Denn diese können schon heute sehr leicht gefälscht werden. Mit auf den Fingerspitzen applizierten künstlichen Fingerabdrücken könnten etwa automatisierte Grenzkontrollen leicht umgangen werden.

3.9. Bibliotheken

Auch für Bibliotheken wird RFID zunehmend interessanter, um die Effizienz zu steigern oder die Kosten zu reduzieren, bzw. neue Serviceleistungen für ihre Kunden anbieten zu können. Bedienung und Instandhaltung lassen sich automatisieren. Wenn Benutzer einen ganzen Bücherstapel auf eine Ablage legen und ein System automatisch sekundenschnell alle Bücher als ausgeliehen oder zurückgebracht verbucht, so steckt eine fortschrittliche Bibliothekstechnik dahinter, in der Regel in Form von RFID. Die Unterstützung durch RFID für große und kleine Bibliotheken bietet neben einer Optimierung vor allem ein effizientes »Ressourcen-Management« zur Bewältigung der ständig steigenden Anforderungen an Beratung und Service. Mit dem BiblioChipTM System lassen sich (im Vergleich zum Barcode) bei der Ausleihe, bzw. der Rückgabe etwa 85% Arbeitszeit einsparen. Neben einer Effizienzsteigerung geht beim Einsatz vom BiblioChipsTM auch eine zentrale Mediensicherung mit den BiblioChipsTM einher. Einfache Sicherungsschleusen an den Ausgängen prüfen, ob die Medien korrekt registriert wurden. Ist dies nicht der Fall, wird ein Alarmsignal ausgelöst.

Ein weiterer großer Vorteil, der erst durch Technologien wie RFID ermöglicht wird, ist dass die Medien nicht nur lokal, sondern auch an vielen Orten in der Stadt an so genannten Rückgabeautomaten wieder abgegeben werden können.

3.10. Lager

RFID-Lesegeräte registrieren die mit den Chips ausgestatteten Produktpaletten beim Transport im Lager. Hierdurch sind stets die Anzahl der gelagerten Produkte und ihr aktueller Lagerplatz bekannt. Dadurch entfällt zeitraubendes Suchen, die Technik erfasst zu erwartende Produktengpässe und ermöglicht eine rechtzeitige Nachbestellung. Lagerbestände lassen sich abbauen und Lagerkosten reduzieren, da sich die Waren rechtzeitig bei den Zulieferfirmen ordern lassen. Da das RFID-System auch Lagerein- und -ausgänge erfasst, lässt sich auf dieser Basis das Lagermanagement effizient gestalten. Das spart Zeit und Kosten.

RFID-Systeme sind automatische Identifikationssysteme, mit denen Daten berührungslos aus Etiketten gelesen und bei manchen Systemen auch in sie geschrieben werden können. RFID-Etiketten besitzen Mikroprozessoren oder hochminiaturisierte Logikschaltungen, und sie arbeiten im Allgemeinen ohne eigene Energiequelle. Sie lassen sich daher unauffällig an oder in Objekten aller Art unterbringen und sogar in Mensch und Tier implantieren. Über Lesegeräte können angeschlossene Systeme Objekte und Personen weltweit eindeutig identifizieren. So ermöglicht die RFID-Technologie beispielsweise, Warenflüsse vom Erzeuger bis an die Ladentheke oder sogar bis in den Haushalt der Kunden zu verfolgen.

Lagersysteme werden aufgrund einer Vielzahl unterschiedlicher Gründe gebildet:

- Unregelmäßige Zu- und Abgänge (z. B. zwischen Fertigung und Distribution)
- Mengenausgleich, beispielsweise im Rahmen der Fertigung wirtschaftlicher Losgrößen
- Sicherstellung der Auslastung kostenintensiver Produktionsanlagen (bei Störungen, Lieferengpässen, Verkehrsproblemen usw.)
- Nutzung kostenoptimierter Bestellmengen durch die Gewährung von Rabatten
- Saisonale Schwankungen im Absatzverhalten
- Schaffung eines hohen Lieferservice durch schnelle Befriedigung von Aufträgen oder Kundenwünschen bzw. Sicherung der Lieferfähigkeit insgesamt
- Lagerung zur Wertsteigerung (durch Reifung) oder zwecks spekulativer Absichten
- Erfüllung von Zusatzaufgaben (zB Bereitstellung zur Kommissionierung)

Produktpaletten werden im Lager mit Chips versehen und von RFID-Lesegeräten registriert. Dadurch sind jederzeit die Anzahl der Produkte und deren Lagerplatz abrufbar. Nachbestellungen von Produkten und Suchvorgänge werden dadurch erheblich erleichtert, Lagerbestände und Lagerkosten sind genauer und kostengünstiger zu kalkulieren. Auch Nachbestellungen von Produkten können effizienter vorgenommen werden, da ein RFID-System auch die Lagerein- und ausgänge registriert.

Unit-Tagging

Unter Unit-Tagging wird die Bestückung von logistischen Einheiten und/oder Versandeinheiten mit einem Transponder verstanden. Der Transponder trägt eine eindeutige Seriennummer, wodurch jede Versandeinheit eindeutig identifizierbar ist. Mit dieser Seriennummer kann eine Abfrage gestartet werden, welche den Inhalt der Versandeinheiten sowie zusätzliche Informationen zurückgibt. Das Einsatzfeld des Unit-Taggings erstreckt sich vom Warenausgang beim Hersteller bis hin zum Wareneingang in den Filialen.

Item-Tagging

Unter Item-Tagging wird die Verwendung von RFID-Transpondern auf Artikel- bzw. SKU-Ebene (SKU = kleinste bestandsführende Lagereinheit; Stock Keeping Unit) verstanden. Item-Tagging ermöglicht eine genaue Identifizierung der Einzelteile und sichert die Rückverfolgbarkeit.

So genannte hochdynamische, automatische oder bewegliche Lager- und Kommissionierungssysteme existieren bereits. Hier handelt es sich meistens um horizontalbewegliche Regelkarusselle. Auf diesen können bis zu 20.000 Behälter appliziert werden. Automatische Hebevorrichtungen können pro Stunde bis zu 2.000 Ein- und Auslagerungen (Doppelspiele) der Behälter durchführen. Durch Förderbänder werden die Waren in Kunststoffboxen zu den Kommissionierungsstellen transportiert. Die Behälter sind mit passiven RFID-TAGS versehen. An gewissen Stellen der Förderbänder wiederum befinden sich Lesegeräte, die automatisch erfassen wo im Lager sich Waren und Behälter befinden. Dadurch kann die Ware jederzeit lokalisiert werden. So ist es möglich die Daten der Warenbehälter und des Lagerverwaltungssystems mit den Auftrags- und Kommissionierungsdaten zu verknüpfen und dadurch jede Unregelmäßigkeit sofort zu erfassen.

Gegenüber herkömmlichen Lagersystemen erreicht man dadurch eine bis um das zehnfache gesteigerte Kommissionierungsleistung, die doppelte Lagerverdichtung und eine hohe Ersparnis an Wegzeiten.

Bei einem auf RFID aufgebauten Staplersteuerungs- und Chargenverfolgungssystem eines großen Getränkeherstellers in der BRD basiert die Positionsbestimmung auf 2.500 im Lagerboden eingelassenen RFID-Tags. Die Ortung der Lagerplätze erfolgt durch RFID-Tags, Strichcodes an Paletten und in die Stapler eingebaute Scanner. 30 Gabelstapler im Lager leisten ca. 4 Millionen Palettenbewegungen im Jahr. Bis zu 600 LKWs am Tag können beladen werden. Nach Angaben des Getränkeherstellers habe es bislang keinen Systemausfall gegeben und die Leserate liege bei 100%. Die Einsparung pro Jahr durch Verzicht auf das Einscannen der Paletten per Hand beziffert das Unternehmen bereits jetzt auf 250.000 Euro (BRD, Lebensmittelzeitung vom 16.09.2005)

3.11. Logistik

Eine Logistikkette funktioniert, wenn zum erforderlichen Zeitpunkt die bestellten Waren fertig zur Auslieferung und in ausreichender Menge am vorgesehenen Platz lagern und die Daten verfügbar sind.

RFID soll die gesamte Lieferkette – vom Produktionsort bis ins Regal – überwachen. Ziel ist es, zu jedem Zeitpunkt erfassen zu können, in welchem Abschnitt der Supply Chain (Lieferkette) sich ein Produkt oder eine Palette gerade befindet. Zähl-, Such- und Sortierprozesse durch Arbeitskräfte entfallen.

Warenein- und -ausgänge, Nachbestellungen aus den Geschäften, Lieferungen in die Märkte, der Abgleich von Bestell- und Lieferdaten, das Ausstellen von Empfangsbestätigungen sowie Wareneingangsbuchungen etc., all das lässt sich automatisch kontrollieren und steuern.

Wo auch immer sich die Palette befindet, ist sie erst einmal gechippt, dann ist sie jederzeit zu orten: Beim Hersteller oder Lieferanten, im Lkw auf dem Transport oder am Ziel, beim Käufer/Händler im Zwischenlager oder im Supermarkt, im Kaufhaus oder …

In Regalen eingebaute Lesegeräte können automatisch das Einräumen und die Entnahme von Waren oder die Überschreitung des Haltbarkeitsdatums von Produkten erfassen. Zähl-, Such- und Sortierprozesse durch Arbeitskräfte entfallen auch hier. Leicht verderbliche Waren können rechtzeitig aus dem Verkauf genommen werden. Damit kann RFID-Technik einen Beitrag zur Qualitätssicherung und -verbesserung leisten. Auch die Out-of-Stock-Rate (Regallücke) lässt sich reduzieren. Im Frischebereich lässt sich lückenlos die Produkttemperatur verfolgen und somit der Qualitätsstandard hochhalten. Die Informationen über die Waren lassen sich wiederum mit den Daten des Warenwirtschaftssystems abgleichen. Dieses sortiert automatisch Produkte aus oder fordert neue Waren an. Neben der Möglichkeit einer eindeutigen Identifizierung von Produkten und Paletten ist eine lückenlose Rückverfolgung der Herkunft und des Transportwegs der Waren möglich. Jede Station entlang der Produktionskette hinterlegt auf dem Chip die entsprechenden Daten und Informationen. Dies erleichtert auch die gesetzlich verankerte Rückverfolgbarkeit und evtl. notwendige Rückrufaktionen von Lebensmitteln (entsprechend den gesetzlichen Vorgaben der EU-Verordnung 178/2002).

90 Prozent der Food-Lieferanten von „Marks & Spencer" (M&S) – einer britischen Kette, die Kühl- und Trockensortimente in Mehrweg-Transportbehältern verschickt, tauschen bereits heute RFID-basierte Daten mit dem Händler aus. Der Einsatz von RFID hat nach Angaben von „M&S" die Zusammenarbeit mit den Zulieferern, den Überblick über die Bestände sowie das Rechnungswesen verbessert und gleichzeitig den Aufwand für Administration und Suche nach bestellter Ware reduziert. Die Lieferkette bei „M&S" beispielsweise kommt folgendermaßen in Gang: Ein Food-Lieferant erhält eine Order. Die Kommissionierbehälter werden befüllt und Daten wie Gewicht, Preis und Mindesthaltbarkeitsdatum als Barcode im IT-System des Lieferanten hinterlegt. Hier werden auch die Bestellung und die vorgesehene Lieferung miteinander abgeglichen und die RFID-Tags beschriftet. Beim Warenausgang rollt die Lieferung an einem RFID-Lesegerät vorbei. In den Distributionszentren von „M&S" werden Ein- und Ausgang der Behälter ebenfalls per RFID registriert. Damit lassen sich Abweichungen zwischen bestellten, verschickten und gelieferten Warenmengen sofort ermitteln. „M&S" weiß genau, welche Waren sich wo befinden, egal ob in einem Lkw oder bereits in einem Distributionszentrum (vgl. Lebensmittelzeitung vom 30.9.2005). Die Warenausgangs- und Eingangskontrolle erfolgt automatisch, ohne dass Listen per Hand oder teilautomatisiert abgeglichen werden müssen.

Geht es nach dem Willen der Industrie, so soll in Zukunft jede einzelne Verkaufseinheit gekennzeichnet sein. Jede Packung kann dann bei ihrem Lauf durch die Lieferkette verfolgt, der Bestand der Produkte im Supermarktregal optimiert und ihr Haltbarkeitsdatum kontrolliert werden. RFID in der Logistik ermöglicht einen hohen Grad an Transparenz über den Standort und den Verbleib von Produkten. Zeitnahe und bedarfsgenaue Bestellungen sind möglich. Es entstehen fortlaufende Daten, frei von Abweichungen, zentral erhoben und verarbeitet.

3.12. Tickets zur Fußball-WM

Das Organisationskomitee der Fußball-WM 2006 hat den Zugang zu den Veranstaltungen in den zwölf deutschen WM-Stadien durch Smart Labels mit RFID gesichert. Dazu sind die Tickets mit Chips ausgestattet. Durch die Verbindung von personalisierten RFID-Labels und elektronischer Zugangstechnik war sichergestellt, dass nur berechtigte Personen Zutritt zum Stadion erhielten, Ticketfälschungen waren erschwert und der Schwarzhandel unterbunden.

3.13. e-card: Die österreichische Gesundheitskarte

Die österreichische „e-card" (SV-Chipkarte) ist die personenbezogene Chipkarte des elektronischen Verwaltungssystems der österreichischen Sozialversicherung (Kranken-, Unfall-, Pensions-, Arbeitslosenversicherung). Dieses System hat die Verwaltungsabläufe zwischen Versicherten, Dienstgebern, Vertragspartnern (Ärzten, Spitälern, Apothekern usw.) und diesen gleichgestellten Personen sowie Sozialversicherungsträgern zu unterstützen. Es ist so zu gestalten, dass die von den Sozialversicherungsträgern zu vollziehenden Gesetze weitgehend ohne papierschriftliche Unterlagen vollzogen werden können. Neben den e-cards werden auch o-cards zur Kennzeichnung ärztlicher Ordinationen ausgestellt, weitere Kartenarten (a-card für Apotheken etc.) werden überlegt.

Die e-card gehört zum österreichischen E-Government. Sie verwendet elektronische Signaturen und ist keine reine Krankenversicherungskarte (Gesundheitskarte), sondern eine allgemein nutzbare Chipkarte. Mit ihr ist auch außerhalb der Sozialversicherung die elektronische Authentifizierung der Kartenbesitzer möglich, die Karte bietet sicheren Zugriff auf persönliche Daten, die bei anderen Stellen gespeichert sind.

Das e-card-System ist ein on-line-System, über welches Versicherungsansprüche sofort verifiziert werden können (einschließlich Nebenangaben wie Rezeptgebührenbefreiungen etc.). Für den Fall, dass keine Leitungsverbindung zum zentral geführten Rechenzentrum hergestellt werden kann, ist es off-line möglich, versicherungsrelevante Angaben (Arztbesuche) zu speichern und nach Wiederherstellung der Verbindung zu übertragen.

Die e-card gilt für alle gesetzlichen Krankenkassen, darüber hinaus auch für eine Reihe von Beamten-Sondersystemen. Versicherungswechsel berühren die Verwendbarkeit nicht. Einrichtungen für die Aktualisierung der Kartenangaben sind nicht notwendig. Angaben über Versicherungsschutz (Versichertenstatus bei welcher Krankenkasse, Gebührenbefreiungen usw.) sind nicht auf der e-card gespeichert, sondern werden mit der Karte festgestellt. Diese Vorgangsweise vermeidet es, dass Versicherungsschutz von den Angaben auf einer (möglicherweise defekten, verlorenen usw.) Karte abhängt und erspart gesonderte Sicherungssysteme für diese Fälle. Für solche Situationen bestehen Vereinbarungen, die bis zu einer Abrechnungsgarantie zugunsten des Arztes reichen können. Wer nicht versichert ist, behält die e-card und kann sie für andere Zwecke weiter verwenden (z. B. als Bürgerkarte, zur Dokumentation der Personendaten), eine neue Versicherung wird (beim Arzt usw.) mit derselben Karte dokumentiert.

Die e-card wird wie ein Schlüssel verwendet, auf ihrem Chip sind und werden keine medizinischen Daten gespeichert. Technisch wäre das möglich und könnte – sofern datenschutzrechtliche Bedenken ausgeräumt werden können – in einer weiteren Ausbaustufe auf freiwilliger Basis erfolgen. Das gilt insbesondere für die bereits gesetzlich vorgesehene Speicherung von Notfalldaten auf dem Kartenchip. Die dafür notwendige Durchführungsverordnung des zuständigen Bundesministers ist noch nicht erlassen, weil auch 2007 noch eine Reihe grundlegender Fragen offen sind: Die Behandlung im Notfall darf z. B. nicht davon abhängen, ob eine Chipkarte - lesbar - vorhanden ist, auch die Aktualität der darauf gespeicherten Daten muss verifizierbar sein.

Der Chip der e-card erfüllt die Anforderungen, die im Behördenverkehr und im Wirtschaftsleben an ein Bürgerkartensystem zu stellen sind (rechtsverbindliche Unterschriftsmöglichkeit durch elektronische Signatur aufgrund eindeutiger Identifikation des Menschen, auf den die Karte ausgestellt ist). Dadurch ist auch die Abfrage personenbezogener Daten über Internet (einschließlich Telebanking, Steuererklärung usw.) vorbereitet bzw. in Teilbereichen bereits möglich (Versicherungskontoabfrage, Steuererklärungen), ohne dass für jede Abfragemöglichkeit mit gesonderten PINs, TANs, Passwörtern usw. gearbeitet werden muss. Der dadurch mögliche Entfall der Benutzerverwaltung bringt auch den Anbietern solcher Dienste nennenswerte Erleichterungen. Die Bürgerkartenfunktion einer e-card kann von jedem Internet-PC mit signaturfähigem Kartenlesegerät genützt werden.

Auf dem Chip und auf der Karte selbst sind folgende Daten verzeichnet:

- Kartenfolgenummer (wenn - nach Verlust - usw. mehrere Karten mit den gleichen Daten für einen Menschen ausgestellt wurden)
- Vorname(n)
- Familienname(n) (auf dem Chip in zwei Varianten: mit und ohne diakritische Zeichen)
- Geburtsdatum
- Akademischer Grad
- Kennnummer des Sozialversicherungsträgers
- Kennnummer der Karte
- Ablaufdatum
- Sozialversicherungsnummer

Mit einem handelsüblichen Chipkartenleser und entsprechender Software, wie z. B. die Software der Bürgerkarte oder anderer Tools, können diese Daten vom Chip ausgelesen werden. Auf der Rückseite der e-card befindet sich die Europäische Krankenversicherungskarte EKVK, auch European Health Insurance Card EHIC genannt, die den Auslandskrankenschein ersetzt.

Zusatzanwendungen außerhalb des Gesundheitsbereiches

Neben den Anwendungen im Gesundheitsbereich kann die e-card zur Bürgerkarte aufgerüstet werden. Dafür werden (teilweise in Zusammenarbeit mit den Anbietern von Chipkartenlesegeräten) Werbeaktionen im Rahmen öffentlicher Veranstaltungen (Messen usw.) durchgeführt.

Weitere privatwirtschaftliche und öffentliche Anwendungen sind in gesetzlichem Rahmen auch außerhalb der Sozialversicherung möglich, für die Verwendung der e-card sind entsprechend den gesetzlichen Vorgaben (Ersatz des Mehraufwandes) Zahlungen an den Hauptverband der österreichischen Sozialversicherungsträger zu leisten.

4. IM HANDEL HAT DIE ZUKUNFT BEREITS BEGONNEN...

Noch stellen Kundinnen und Kunden ihren Einkauf im Laden selbst zusammen, legen alles auf das Förderband, lassen die Preise vom Kassenpersonal durch eine elektronische Kasse erfassen, bezahlen und packen.

Glaubt man einigen Experten, so steht dem deutschen Einzelhandel eine zweite Selbstbedienungswelle – diesmal an der Kasse – bevor. Demnach werden schon in fünf Jahren Kundinnen und Kunden weltweit Artikel im Wert von 1,3 Billionen (!) Dollar ohne die Hilfe von Kassiererinnen und Kassierern erwerben, zehnmal soviel wie derzeit. Und dies auch mit alter Technik, der Barcodekennzeichnung an den Waren.

Die Kunden haben gelernt, die Ware selbstständig zu prüfen und abzuwiegen. Geht es nach dem Willen der Industrie, dann lernen sie jetzt auch noch das selbständige Bezahlen an der Kasse.

Die USA zeigt, wie das geht:

Dort bietet bereits jeder dritte Supermarkt so genannte Self-Checkout-Kassen an, an denen die Kundinnen und Kunden den Inhalt des Einkaufswagens per Strichcode und Infrarot-Scanner zu erkennen geben. Bezahlt wird anschließend per Kreditkarte oder am nebenstehenden Bargeldautomaten. Betrug ist kaum möglich, denn das Kassensystem wiegt die eingescannten Artikel automatisch und eine Aufsichtsperson überwacht zusätzlich die Kassiervorgänge an meist vier parallelen Abrechnungsstellen.

Die amerikanische Baumarktkette „Home Depot", die in über 1.000 Märkten knapp 4.200 Self-Scanning-Kassen aufgestellt hat, will zudem eine gestiegene Kundenzufriedenheit festgestellt haben. Fast zehn Prozent der Kundinnen und Kunden sollen laut Umfrage eines Marktforschungsunternehmens den Einkauf im Home Depot gerade wegen der Selbstzahlerkassen gewählt haben. Der US-Handelskonzern „Supervalu" vermeldet, dass sich die Investition in die Self-Checkout-Kassen bereits nach zwölf Monaten ausgezahlt habe. Der Lebensmittelhändler hatte die elektronischen Kassen in 60 seiner Läden installiert, um gegen den Konkurrenten „Wal-Mart" bestehen zu können.

Bemerkenswert ist, dass der Kassiervorgang bei Kundinnen/Kunden rund zweieinhalb Mal so lange dauert, als bei einer/-m routinierten Kassierer/-in. Die beim Kassieren selbst aktiven Kundinnen/Kunden empfinden aber offensichtlich diese Zeitspanne als kürzer.

Noch nie zuvor waren die Erwartungen des Einzelhandels so groß, die Warteschlangen an den Kassen ohne steigende Personalkosten beseitigen zu können. Die Chancen stehen gut: Neue Systeme, die sich stärker an den Gewohnheiten der europäischen Konsumentinnen und Konsumenten orientieren, sind neu auf den Markt gekommen. Rund 70 Prozent aller Kunden benennen die Warteschlangen vor den Kassen als das schlimmste Ärgernis im Einzelhandel, berichtet das Euro-Handelsinstitut (EHI). „Der Kassengang ist der letzte Eindruck, den der Kunde von Ihrem Geschäft hat«, sagt Michael Gerling, Geschäftsführer des EHI (vgl. Lebensmittelzeitung vom 10. Februar 2006).

Dies sei Grund genug, sich mit seiner Automatisierung zu beschäftigen. Attraktiv ist zudem, dass bis zu 50 Prozent der Personalkosten des Lebensmittel-Einzelhandels in die Arbeit an der Kasse fließen. Werden die Strichcodes durch RFID-Funketiketten ersetzt, lässt sich der zeitliche Aufwand deutlich weiter reduzieren, weil die Kundinnen und Kunden dann nur noch mit ihrem Einkaufswagen mit dem kompletten Einkauf durch die Scannerschleuse fahren und die Waren vom System registriert werden. Die Zahlung kann per Karte, am Bargeldautomaten oder in Zukunft auch per Fingerabdruck erfolgen. Letzteres setzt lediglich voraus, dass die Kundinnen und Kunden im Geschäft ihren biometrischen Fingerabdruck hinterlassen.

4.1. Zukunftsszenario: Einkaufen

Zukunftsszenario: Einkaufen

So könnte ein nicht sehr fernes Szenario aus der Einkaufswelt der Zukunft aussehen: Eine Kundin nimmt eine Jacke aus einem intelligenten Regal. Ein Plasma-Werbebildschirm macht daraufhin die Interessentin auf die passende Hose oder den zugehörigen Rock aufmerksam und bietet ihr einen günstigen Kombipreis an. Bei der Anprobe ermöglichen Funketiketten in der Kleidung, dass die Kundin außerdem farbliche Varianten des Modells oder passende Accessoires per Bildschirm offeriert bekommt. Entscheidet sie sich zum Kauf, so passiert sie eine Schranke, wo nach Einlesen der RFID-Chips auf den Artikeln direkt die Abbuchung von der Kreditkarte veranlasst wird. Dazu muss die Kundin die Sachen nicht einmal mehr aus der Tasche nehmen. Mit Verkaufs- oder Kassenpersonal kommt die Käuferin nicht in Kontakt. Personal bleibt beim Einkauf weitgehend unsichtbar und hat vorwiegend Aufsichtsfunktion. Nur falls die Abbuchung nicht reibungslos klappt, kommt eine Überwachungskraft, die die Ausgangsschleusen per Bildschirm im Blick hat, zu Hilfe. Das stetige Nachpacken von Ware übernehmen ferngesteuerte technische Einheiten, die an der Decke entlangfahren. Menschen kontrollieren und ordnen allenfalls die Warenströme, den bargeldlosen Zahlungsverkehr und verwalten Datenbanken. In einer solchen Datenbank ist dann auch die Käuferin der Markenkleidung registriert, sie wird künftig automatisch mit entsprechenden Werbebotschaften versorgt. Wenn beim Verlassen des Kaufhauses keine Deaktivierung der RFID-Etiketten erfolgt, ist noch Jahre später verfolgbar, wann die Jacke durch wen wo gekauft wurde und bei welchem Entsorger sie schließlich im Müll landete.

Im Handel tätige Unternehmer/-innen, Firmenvorstände und Lieferanten aus der Konsumgüterindustrie erwarten von der Funktechnik RFID einen Produktivitätsschub und eine Umwälzung des Handelsalltags. „RFID wird unsere Branche in den nächsten 10, 15 Jahren verändern«, prognostiziert Zygmunt Mierdorf, Vorstandsmitglied und IT-Chef der „Metro Group". Der Metro-Vorstands- vorsitzende Dr. Hans-Joachim Körber hat klare Rationalisierungsziele: Die Funktechnik soll helfen, „effizienter zu werden und alle versteckten Reserven der Lieferkette zu erschließen«.

Ähnliches hat auch der Rewe-Vorstandssprecher Dr. Achim Egner im Sinn: »Mit RFID können wir einen Quantensprung bei der Verbesserung unserer Geschäftsprozesse erreichen«. In den nächsten zwei, drei Jahren soll der Einsatz von RFID im Handel die Logistik automatisieren, was Arbeitskräfte einspart. Außerdem lassen sich die Bestände besser überblicken, letztendlich um diese senken zu können und trotzdem weniger Regallücken zu haben.

Mittelfristig dient RFID der Rationalisierung und Optimierung im Warenverkehr. Längerfristige Ziele sind die lückenlose Kontrolle jeder einzelnen Ware mittels eines EPC.

In der Organisation »EPCglobal Inc.«, die das Modell und die Standards für den branchenweiten Einsatz von EPC-RFID entwickelt, sind viele der weltgrößten Handelskonzerne und Konsumgüterhersteller vertreten. Nicht jeder RFID-Einsatz hat etwas mit EPC zu tun – doch wenn es in der Konsumgüterlogistik und im Handel um RFID geht, dann um das Modell des EPC-Netzwerks und seine Chancen, sich nicht nur in einzelnen Unternehmen, sondern in der ganzen Branche weltweit durchzusetzen. Zur Vision von »EPCglobal Inc.« gehört der RFID-Tag an jeder Produktpackung, der den vollautomatischen Check ohne Kassierer/-in ebenso ermöglicht wie den Alarm, wenn eine Ware im Regal zur Neige geht.

4.2. Pilotversuche im Handel

Die ersten Schritte des Handels mit RFID scheinen der- zeit noch weit entfernt von dem technisch denkbaren EPC-Einsatz. Jedoch nutzen »Wal-Mart«, »Metro Group«, »Rewe«, »Otto Versand«, »Marks & Spencer« u.a. bereits in Pilotversuchen und ersten Roll-outs (Markteinführungen) RFID, um klassische Scanner in der Logistik und Warenannahme zu ersetzen.

Der weltweite Handelskonzern „Wal-Mart" ist der Einzelhändler, der heute mit RFID in den USA am weitesten ist. Bereits 300 seiner größten Lieferanten schicken ihre Waren mit Transpondern an Umkartons oder Paletten an fünf Distributionszentren (DCs) des Handelsgiganten im Süden der USA. Diese fünf DCs beliefern dann rund 500 Filialen von „Wal-Mart" und „Sam's Club" mit teilweise getaggten logistischen Einheiten (Waren). Der US-Konzern hat angekündigt, die Zahl seiner Stores mit RFID-Lesegeräten bis Januar 2007 auf 1000 zu verdoppeln. Bis dahin sollen weitere 300 Hersteller Funk-Tags an ihren Waren befestigen. Die bisher bei „Wal-Mart" im Vergleich zu Nord- und Westeuropa rückständige Logistik erklärt das Tempo: US-Händler lassen überwiegend einzelne Kartons mit Ware per Hand in die Lkws tragen, während in Europa üblicherweise ganze Paletten mit Strichcode verladen werden.

4.3. Vorreiter Metro und Rewe

Die „Metro Group" (Metro C+C, Real, Extra, Kaufhof, Media-Saturn) ist RFID-Vorreiter in Europa. Heute nutzt Metro RFID-Lesegeräte in neun Lagern und 13 Märkten.

Noch vor Ende 2006 sollen es über 200 Lokationen (Standorte) sein. Ebenfalls bis Ende des Jahres will „Metro Group" mit RFID-Tags an Kartons (Handelseinheiten/Gebinden) starten. Zusätzliche Funketiketten auf den Umkartons jeder einzelnen Ware ermöglichen es, nachzuvollziehen ob gelieferte Ware noch in einem Lagerraum liegt oder bereits zum Einräumen auf die Verkaufsfläche geschafft wurde. Auf Basis der bereits getaggten Paletten rechnet die Düsseldorfer „Metro Group" damit, mittels RFID die Kosten im Wareneingang um bis zu 17 Prozent zu senken, den Warenschwund um bis zu 18 Prozent zu verringern und die Regallücken (Out-of-Stocks) je nach Sortiment um 9 bis 14 Prozent zu reduzieren. Nach Metro-Angaben ist die Zeit, um eine Palette am Wareneingang der Lager anzunehmen und an den vorgesehenen Lagerplatz zu befördern, von bisher 90 auf nur noch 70 Sekunden gesunken. Beim Abgleich einer ganzen Lkw-Ladung sinke der Zeitaufwand der Lagerarbeiter/-innen von 15 auf drei Minuten. Praktisch bedeutet dies, dass ein Handelsunternehmen, das vorher fünf Lagerarbeiter/-innen benötigte, nun mit einer Kraft auskommt. (Diese, in einer Studie im Auftrag der „Metro Group" ermittelten Werte, wurden im Rahmen der Metro-Lieferanten-Konferenz am 9. Juni 2005 in Köln mitgeteilt.)

Ein weiteres deutsches Handelsunternehmen, die „Rewe Group", erhält seit März 2006 von ihren Lieferanten Paletten mit RFID-Tags. Mindestens 30 Hersteller sind an diesem „Pilot-Roll-out" im Rewe-Lager Norderstedt bei Hamburg beteiligt. „Rewe Group" ist bereits seit längerem dabei, ihre Informationstechnologie (IT) so einzurichten, dass die logistischen Prozesse zunehmend automatisch ablaufen. „Rewe Group" nennt dies Ereignissteuerung und meint damit, dass Geräte automatisch reagieren, wenn ein bestimmter Prozessschritt abgeschlossen ist oder auch genau dann, wenn er nicht der Planung entspricht. So kann das RFID-Funksignal im Wareneingang selbstständig den Prozess der Warenannahme und Einlagerung anstoßen, also zum Beispiel den Staplerfahrer alarmieren. Oder das RFID erkennt zu bestellende Ware und verschickt automatisch eine E-Mail an den Lieferanten. Ereignissteuerung ist zwar auch mit anderen Mess- und Regeltechniken möglich, RFID ergänzt die automatische Protokollierung der Warenbewegungen jedoch besonders effektiv.

4.4. Jedes Stück ist markiert

Um die RFID-EPC-Daten sowohl bei „Metro Group" als auch bei „Rewe Group" sinnvoll nutzen zu können, müssen die Hersteller den Inhalt jeder Lieferung per EDI angekündigt haben. EDI steht für Electronic Data Interchange und ist der Überbegriff für Industriestandards zum elektronischen Austausch von Geschäftsdokumenten. Zwischen EDI und RFID lassen sich zahlreiche Parallelen feststellen, beide Technologien erleichtern das Auftragsmanagement. Während EDI-Dokumente die Basis für die Erteilung von Aufträgen sind, gibt RFID Einblick in die Dynamik der Lieferprozesse und ermöglicht es, die Effizienz des Vertriebs zu untersuchen. RFID ist dem EDI, dessen Technologie auch bereits ein hohes Datenaustauschvolumen vorweist, jedoch aufgrund der Echtzeitübertragung im Vorteil.

„Metro Group", „Rewe Group" und „Wal-Mart" sowie eine unbekannte Anzahl weiterer amerikanischer Handelsunternehmen nutzen bereits UHF-Funkchips (Ultrahochfrequenz zwischen 860 und 960 MHz) nach den Standards von „EPCglobal Inc." Im Handelsalltag bietet RFID weitere Möglichkeiten: Bereits verwirklicht ist die Kontrolle hochwertiger Ware (etwa Digitalkameras und Handys) auf ihrem Weg durch das Kommissionierzentrum des „Otto-Versands" in Hamburg und die Steuerung des Umlaufs von 4,5 Millionen Mehrweg-Transportverpackungen für Lebensmittel per Transponder durch den britischen Händler „Marks & Spencer". In beiden Fällen handelt es sich zwar um RFID-Systeme abseits der EPC-Standards – die Unternehmen haben aber erklärt, dass sie bei künftigen Projekten vermutlich auch auf EPC setzen werden.

„Marks & Spencer“ etwa testet bereits EPC-Tags an Textilien. Praktisch alle wichtigen Personen im Handel und in der Konsumgüterindustrie bevorzugen den EPC-Standard der Organisation „EPCglobal Inc.“ Das hat zwei wichtige Gründe: Zum einen lassen sich die Kosten für den unternehmensübergreifenden Einsatz entlang der Lieferkette nur begrenzen, wenn alle Beteiligten die gleiche Technik einsetzen. Zum anderen aber locken die mittel- und langfristigen Aussichten des EPC. Die wichtigste Veränderung der Branche ist durch den RFID-Tag auf jeder einzelnen Verpackung und auf jedem Produkt zu erwarten. Das ist die Chance für „EPCglobal Inc.“, da die digitale Struktur des EPC genug Nummern ermöglicht, um jeder Packung einen eigenen Code zu geben. Während der EAN-Barcode nur eine Nummer für jeden Artikel-Typ zulässt, ermöglicht der 96 Bit große digitale EPC zusätzlich das Durchnummerieren jeder einzelnen Verkaufseinheit, also jeder einzelnen Packung Milch oder Kaffee etc.

Durch EPC sowie die RFID-Funkübertragung sollen in 10 bis 15 Jahren Einkäufe ohne Personal an den Kassen möglich und dann auch üblich sein. Auf Werbespots von „IBM“ und „Metro Group“ ist das automatische Bezahlen bereits Thema: Die/Der Kundin/Kunde schiebt den Einkaufswagen am RFID-Lesegerät vorbei, dieses erfasst alle Waren automatisch und bucht den Betrag vom Konto ab. Das ergänzende EPC-System schlägt Alarm bei Diebstahl, sorgt für stets frische Produkte in Kühltruhe und Regal, und es gibt einen Echtzeit-Überblick über die Bestände in Lagern, Filial-Regalen und die komplette Lieferkette von der Fabrik bis in den kleinsten Laden. Die automatisierte Funk-Erfassung von Warentransporten und Beständen ermöglicht es, festgelegte Mengen an Waren weder zu über- noch zu unterschreiten, Abweichungen zu melden und entsprechend umzusteuern.

4.5. Vorsicht ist gut - Kontrolle ist besser

Ein Ziel beim Einsatz von RFID ist die kostensparende Automatisierung der bisher von Menschen ausgeübten Arbeit, mit der Folge, dass Arbeitsplätze verschwinden. Außerdem geht es darum, die Bestände in den Lagern zu senken und dadurch die Menge des gebundenen Kapitals zu verringern. Ferner lässt sich die Überschreitung des Haltbarkeitsdatums automatisch kontrollieren, was Kosten bei den abzuschreibenden Warenbeständen reduziert.

Hersteller, vor allem von Markenprodukten und von Arzneimitteln, sehen die Chance, mittels EPC-Tags an ihren Produkten Fälschungen und Graumarktimporte zu verhindern. Gleichzeitig soll der EPC direkt an der Ware einen bisher fraglichen Zusatznutzen für die Kunden bringen: Der Mikrowellenherd soll automatisch die Ware (im Karton) erkennen und entsprechend erhitzen, die Waschmaschine registriert, was sie wäscht, der Kühlschrank bestellt eigenmächtig, bei der Beschaffung von Ersatzteilen gibt es keine Verwechslungen mehr.

Der nunmehr gläserne Kunde könnte aber auch ungefragt Ergänzungsprodukte angeboten bekommen. In den Geschäften könnte darüber hinaus eine in die Hand genommene Ware bereits durch die Bewegung der RFID-Tags einen Werbespot initiieren und dadurch zum Kauf dieses oder weiterer Produkte (Cross-Selling) verführen.

Bei diesen Aussichten verwundert das Interesse der Konsumgüterindustrie an der Organisation „EPCglobal Inc.“ nicht. Bereits darin vertreten sind: „Wal-Mart“, „Metro Group“, „Rewe Group“, „Carrefour“, „Tesco“, „Ahold“, „Home Depot“ und „Best Buy“, ebenso wie „Procter & Gamble“, „Unilever“, „Nestlé“, „Johnson & Johnson“ und „Kraft Foods“. Dazu kommen zahlreiche Technologie-Dienstleister, das US-Militär (ein Gründungsmitglied von „EPCglobal Inc.“) und seit kurzem auch große Pharma- und Logistikunternehmen. Als Tochterfirma der Standardisierungsorganisation „GS1“ ist „EPCglobal Inc.“ darüber hinaus umfassend in die Strukturen der Konsumgüterbranche integriert.

Noch stehen „EPCglobal Inc.“ und die dort vertretenen Unternehmen am Anfang der gesetzten Ziele und der damit verbundenen Aufgaben. Für die unterschiedlichen Einsatz-Szenarien müssen Funk-Standards definiert werden. Dazu kommen weitere Elemente des bisher nur als Grobkonzept vorhandenen „EPC-Netzwerks“. Das EPC-Grundmodell sieht lediglich vor, dass relativ primitive und deshalb nur einige Cent teure RFID-Tags einzig die digitale Nummer des EPC speichern.

Alle Daten zu diesem Produkt müssen in Datenbanken gespeichert und dann von den Beteiligten der Lieferkette per Internet abgerufen und fortgeschrieben werden. Für dieses EPC-Netzwerk werden Middleware, Information Services (EPCIS) und Discovery Services benötigt, damit die Computer der beteiligten Unternehmen automatisch miteinander kommunizieren können. All das muss noch im Detail standardisiert, teilweise erst noch entwickelt werden. Dazu kommt eine physikalische Hürde: Abhängig von der Frequenz werden elektromagnetische Wellen im UHF- und HF-Bereich von Flüssigkeiten und Metallen abgeschirmt oder verändert. Angesichts dieser noch ungelösten Forschungs- und Entwicklungsaufgaben kann heute niemand mit Sicherheit sagen, ob sich alle Erwartungen der Firmen an RFID und das EPC-Modell erfüllen lassen.

Middleware

Die Middleware ist eine Software und schließt den Informationskreis zwischen der Datenerfassung von Lager- und Transportbeständen mit den IT-Systemen in Unternehmen. EPCIS – (EPC-)Information Services Ort, an dem sich Informationen über ein Produkt befinden. Ein EPCIS (EPC-IS) ist bei allen Handelspartnern verfügbar. Der EPC Discovery Service speichert die Adressen der EPC-IS Server, auf denen Produktinformationen abgelegt sind. Dadurch ist eine Warenrückverfolgung möglich.

4.6. Rationalisierung versus Arbeitsplätze

Die Folgen der RFID-Technik für die Arbeitsplätze im Handel und die Einsparungsmargen werden unterschiedlich eingeschätzt. Personalabbau hängt von verschiedenen Faktoren ab. Wird jedes einzelne Produkt getaggt und übernehmen die Kundinnen/Kunden das Kassieren selbst, indem sie einen Tunnelscanner passieren, so ist Kassenpersonal überflüssig. Eine Aufsichtsperson bleibt, mehrere Kassierer/-innen gehen.

Nur in den Geschäften, in denen die persönliche Bedienung und Beratung der Kunden noch wesentlicher Bestandteil der Verkaufsphilosophie ist, vermag RFID vorerst wenig zu verändern. Glaubt man dem Metro-Vorstand Zygmunt Mierdorf, dann ist in 15 Jahren alles, vom Lieferanten bis zur/zum Kundin/Kunden automatisiert. Mit den Automatisierungen gehen viele Arbeitsplätze verloren. Selbst wenn die erzielten Rationalisierungseffekte teilweise dazu dienen, dort mehr Personal zu beschäftigen, wo es der Wertschöpfung und der Ankurbelung des Verkaufs dient. Im „Metro Future Store" in Rheinberg, einem umgebauten Verbrauchermarkt der „Metro-Group", werden seit März 2003 in einer nach Firmenauskunft weltweit einmaligen Zukunftswerkstatt zusammen mit Partnern aus Handel, IT-, Dienstleistungs- und Konsumgüterindustrie Technologien getestet, die das Einkaufen für Kunden einfacher und bequemer machen sollen (vgl. Erfolgreich in die Zukunft des Handels starten, Willkommen im Future Store, Metro Group, 2004).

Die Zukunft des Handels hat in diesem Markt bereits begonnen: Mit Selbstzahlerkasse, Info-Terminals, die Rezeptvorschläge liefern, intelligenten Waagen, die Äpfel von Birnen unterscheiden können, einem Einkaufberater als Computer am Einkaufswagen, der Produktinformationen und Preise anzeigt, elektronischen Werbedisplays und Preisschildern und selbstverständlich mit RFID-Anwendungen. Auffällig: Trotz des Technikeinsatzes haben die verschiedenen Frische-Theken eine Personalausstattung, die über der üblichen für solche Märkte liegt. In einer Diskussion mit den Verantwortlichen ließ sich erfahren, dass neue Technologien von Kundinnen/Kunden nur dann angenommen würden, wenn der Markt hell und freundlich gestaltet und auch sonst für die Kundinnen/Kunden attraktiv ist. Das Konzept scheint aufzugehen: Umsatz und Anzahl der Kundinnen/Kunden sind deutlich gestiegen; die Kundinnen/Kunden bescheinigen eine hohe Zufriedenheit mit dem Markt; und 80 Prozent der Kundinnen/Kunden gaben nach einem Jahr an, mindestens einmal eine innovative Technologie genutzt zu haben. Der Wermutstropfen liegt in den Erfahrungen und Erkenntnissen, wie sich die Branche insgesamt ent- wickelt und ob sich solche Einzelhandelskonzepte dauerhaft durchsetzen können. Wenn aus Kostengründen Billig-Konzepte Priorität haben und interessante Kombinationen von technischer und menschlicher Dienstleistung auf dem Prüfstand stehen, dann wird erfahrungsgemäß das Personal durch die Technik ersetzt.

4.7. Geht´s der Wirtschaft gut…

Der Handel forciert die Einführung der RFID-Technik, um einerseits Zeit und Kosten einzusparen und um andererseits die Service- und Kundenorientierung zu erhöhen. Die Konkurrenz auf dem Markt ist groß und im globalen Wettstreit ist jede Einsparungsmöglichkeit willkommen, um im Rennen zu bleiben. Daher drängt sich die Frage auf, ob die Interessen der Arbeitnehmer/-innen und der Verbraucher/-innen auf der Strecke bleiben. Die Vorteile, besonders im logistischen Bereich, sind für die Unternehmen nicht von der Hand zu weisen. RFID wird als Problemlöser eingesetzt, um einen besseren Überblick über aktuelle Warenbestände zu haben, indem alle Warenbewegungen direkt verfolgt werden. Aber auch das Tempo, die Transparenz und die bessere Zusammenarbeit in der Logistikkette sind unternehmerseitig oft genannte Vorteile.

Die Warenlagerung kann zu einem großen Teil auf die Straße oder auf die Zulieferer verlegt werden. Die Ladenbetreiber/-innen können die Waren zeitgerecht beim Zulieferer bestellen. Wegezeiten in den Lagern und der Flächenbedarf reduzieren sich. Logistische Probleme, die zu Lücken in den Regalen führen, sollen der Vergangenheit angehören.

Der Bestand ist jederzeit überschaubar und die Bestellungen sind zeitgerecht planbar. Mit RFID-Technik ist der momentane Standort eines jeden Produkts, einer jeden Palette genau lokalisierbar und das Eintreffen von Waren ist voraussehbar. Die Übersicht über Trendwaren, Ladenhüter oder Waren mit drohendem Verfallsdatum ist einfacher. Warenkontrollen und Nachbestellungen übernimmt das intelligente Regal. Routinearbeiten wie Wareneingangs- und Lieferschein-kontrolle laufen künftig ebenfalls vollautomatisch ab. Die Transparenz, die derzeit erst bei Umverpackungen und Paletten möglich ist, wird sich durch das Taggen der einzelnen Produkte ausweiten. Am Ende kassiert sich die Ware selbst ab und statt der Kassierer/-innen genügt ein Minimum an Aufsichtspersonal. Terminals ersetzen den Rat der Verkäufer/-innen und machen ihre Arbeit laut Vorstellung einiger Arbeitgeber sogar besser.

Doch gilt zu Bedenken, die/der Ladenbetreiber/in hat kein Interesse an einer/einem Kundin/Kunden, die/der jahrelang mit dem Kauf eines Kleides/Anzugs zufrieden ist, sondern die/der bald schon wieder mehr einkauft. RFID soll in den Unternehmen Zeit und Geld sparen und die Position gegenüber der Konkurrenz stärken. Heute ist RFID zwar anfangs meist noch nicht kostendeckend, aber eine aussichtsreiche Investition in die Zukunft.

5. RFID-ANWENDUNGEN MORGEN

Einsatzfelder von RFID-Systemen gibt es in fast allen Wirtschaftsbereichen, viele auch im Handel. Die Palette der Anwendungsmöglichkeiten steigt zudem kontinuierlich. Die vielfältig einsetzbare RFID-Technologie wird zur Selbstverständlichkeit in vielen Lebenslagen. Einige Anwendungsmöglichkeiten des Chamäleons RFID, sind nachstehend skizziert, manche sind bereits realisiert. Als das momentan favorisierte Anwendungsgebiet der RFID-Technologie ist wohl das elektronische Kennzeichnungssystem zu nennen; insbesondere die Kennzeichnung und Identifikation von Objekten (Waren) jeglicher Art.

5.1. Polymer-Technik

Als ICs (Integrated Circuits) auf Siliziumbasis ist die Herstellung von RFID-Tags zu teuer für den Einsatz bei Billigartikeln. Es bietet sich daher an, nach kostengünstigeren Herstellungsmethoden zu suchen. Ein möglicher Ansatz ist die Polymer-Technologie, die sich mit leitenden und halbleitenden Kunststoffen und deren Einsatz in der Elektronik beschäftigt. Schaltungen in Polymertechnik können mit herkömmlichen Druckverfahren produziert werden, sie halten wegen der Flexibilität der Kunststoffe hohen mechanischen Belastungen stand, sind billig und können auf nahezu beliebig geformte Oberflächen aufgebracht werden.

Zur Zeit sind die für die RFID-Tags in Polymerelektronik benötigten Technologien teilweise bereits entwickelt und es wird intensiv an der Umsetzung geforscht. Wegen der geringen Herstellungskosten sind auch Einweg-Tags vorstellbar. Die Firma PolyIC aus Erlangen hat im Dezember 2005 einen komplett funktionierenden Tag (135 MHz) vorgestellt, der aus einem Chip in Polymertechnik und einer den IC umgebenden Antennenspule besteht. Anfang 2006 ist es ihnen gelungen, einen 1-Bit-Tag für 13,56 MHz zu entwickeln. Sinnvolle Anwendungen für Polymertechnik sind auch Sensoren, Batterien und Displays. Sie lassen sich in Verpackungen integrieren, um damit relevante Informationen über ein Produkt auf einem ebenfalls integrierten Display anzuzeigen. Würde man zusätzlich einen Transponder integrieren, kann die Information auch auf einem PDA oder einem Handy dargestellt werden. Verbindungen von Polymerelektronik und RFID-Technik bieten also große Chancen in vielen Bereichen.

5.2. UHF-Transponder

Viele Firmen und Forschungseinrichtungen forschen an der Entwicklung von RFID-Systemen im UHF-Bereich um 900 MHz (Europa 865 - 870 MHz, USA 902 – 928 MHz, Japan 952 -955 MHz). In diesem Frequenzbereich haben auch passive Tags deutlich größere Reichweiten, sie sind weniger störempfindlich, und die Datenübertragungsrate ist schneller als bei der 13,56 MHz-Technik. Es gibt aber auch einige Nachteile, die in der größeren Anfälligkeit für Reflektionen und der schlechteren Durchdringung von Medien, speziell bei Wasser, liegen. Das Industriegremium EPC Global hat inzwischen die Testphase eines Standards (EPC Class1/Gen.2) für UHF-Transponder abgeschlossen, was die Interoperabilität dieser Transponder fördert.

5.3. Lokalisierung

Nahezu alle bisher am Markt angebotenen induktiven RFID-Systeme dienen der Identifizierung und Steuerung von Objekten, bzw. der Identifizierung von Lebewesen. Über die reine Identifizierung hinaus bietet eine zusätzliche Positions-, Richtungs- und Bewegungsermittlung eine erhebliche Erweiterung von RFID-Systemen, so dass damit auch völlig neue Anwendungsgebiete entstehen können. So kann damit ein Tag lokalisiert werden, der sich an einem Objekt in einer Flüssigkeit oder einem anderen Medium befindet, das problematisch für Verfahren mit hochfrequenten elektromagnetischen Wellen ist (Backscatter-Verfahren/UHF-Tag). Es ist allerdings nicht ganz einfach, die Lokalisierungsprinzipien praktisch umzusetzen, die Zusammenhänge magnetischer Wechselfelder und die geometrischen Beziehungen der sie erzeugenden Antennen sind komplex. Mitarbeiter am Lehrstuhl für Informationstechnik (LIKE) der Universität Erlangen-Nürnberg und am Institut für Elektrische Messtechnik und Grundlagen der Elektrotechnik (EMG) der TU Braunschweig können bereits erste erfolgreich abgeschlossene Forschungsergebnisse vorweisen.

5.4. Erfassen von Personen

Nicht nur Waren, auch Personen lassen sich mit aktiven RFID-Tags lokalisieren: So beispielsweise Arbeitskräfte auf einer Bohrinsel, um sie im Falle eines Unfalls schneller finden und retten zu können. Die Tags senden dazu fortlaufend Signale. Anders als bei einer Zutrittskontrolle werden die Beschäftigten dann nicht an einzelnen Zutrittspunkten registriert, sondern sind – ähnlich wie beim GPS-Prinzip – fortlaufend auf einem Bildschirm zu orten.

5.5. Kombination mit biometrischen Verfahren

Zutrittskontrollen über den RFID-Chip sind möglich und lassen sich zudem mit weiteren Authentifizierungsmaßnahmen koppeln, wie zum Beispiel mit zusätzlichen PIN-Eingaben oder mit biometrischen Verfahren wie dem Fingerprint. Diese Technik ist geeignet, um herkömmliche Zutritts- und Zeiterfassungssysteme zu ersetzen.

Per Fingerabdruck

Bei der Bezahlung per Fingerabdruck handelt es sich um ein System, bei dem die Kundeninnen/Kunden ohne Karte, Pin oder Unterschrift bezahlen. Sie müssen sich dazu vorher in ihrem Markt registrieren lassen. Dabei werden die erforderlichen Daten und ein Muster des Fingerabdrucks erhoben und gespeichert. Bei dem Fingerabdruck handelt es sich nicht um ein Bild, sondern um die Aufzeichnung der Position relevanter Punkte der Fingerlinien, die mathematisch umgewandelt und verschlüsselt gespeichert werden. Mit der Registrierung ermächtigen die Kundinnen und Kunden das Geschäft zur Abbuchung künftiger Forderungen vom Girokonto. Um die anfallenden Rechnungen im Laden zu bezahlen, bestätigen die Kundinnen/Kunden beim Einkauf die Richtigkeit des Rechnungsbetrags durch Auflegen des Fingers auf einen Scanner.

5.6. Kennzeichnen von Produkten und Gegenständen

Behältnisse, zum Beispiel mit toxischen Substanzen, lassen sich per Chip eindeutig kennzeichnen. Auch bei medizinischen Produkten wie Medikamenten oder Blutkonserven ist das möglich. Weitere Informationen lassen sich speichern, wie zum Beispiel ein Echtheitszertifikat, das Auskunft über die Qualität des Produktes gibt. Transponder in Berufsbekleidung (bei Feuerwehrleuten, Pflegepersonal, Ärzten etc.) ermöglichen eine zeitsparende automatische Authentifizierung.

5.7. Kriminalität

Auch in Menschen werden mittlerweile Chips implantiert. Beispielsweise hat die mexikanische Regierung kriminelle Aktivitäten in einer zentralen Datenbank des staatlichen Informationszentrums gespeichert. Mit der Begründung, die dort Beschäftigten und das Zentrum selbst schützen zu wollen, wurde allen Beschäftigten ein Chip in den Arm implantiert. Die Regierung behauptet sich mit der Maßnahme insbesondere im Zugangsbereich mehr Sicherheit zu erhoffen.

Für den Handel ist es interessant, die RFID-Technik gleichzeitig als Diebstahlssicherungssystem zu verwenden. Mit Tags gesicherte elektronische Geräte wie Beamer oder Notebooks etc. lassen sich jederzeit orten und bei Diebstahl finden. Im Logistikbereich ist es zudem möglich, zu jedem Zeitpunkt des Transports festzustellen, auf welchem Lkw sich eine Palette mit einem konkreten Produkt gerade befindet.

5.8. Personalausweise

Einführung des elektronischen Personalausweises in der BRD (ePA) Am 23. Juli 2008 hat das Bundeskabinett der BRD die Einführung des elektronischen Personalausweises beschlossen, der ab 1. November 2010 den bisherigen Personalausweis ablösen soll (Gesetzentwurf[9]).

Neu ist das Scheckkartenformat, ein Chip mit PIN (einmalige Zusatzgebühr[10]) und die digitale Speicherung der Fingerabdrücke des rechten und linken Zeigefingers, wobei der Bürger die Wahl haben soll, ob seine Fingerabdrücke gespeichert werden.[11] Damit unterscheidet sich der ePA klar vom ePass, in dem die Abgabe des Fingerabdrucks Pflicht ist. Neu gegenüber den bereits im ePass (→Reisepass) gespeicherten Daten ist jedoch, dass diese Daten auch von den gemeindlichen Meldebehörden geändert werden können. Dies ist beispielsweise bei einem Umzug notwendig, damit kein neuer Personalausweis beantragt werden muss.

Weiterhin wird der Ausweis einen elektronischen Identitätsnachweis bieten, der es ermöglicht, sich mit dem Ausweis und einem besonderen Lesegerät über das Internet elektronisch auszuweisen. Zusätzlich kann eine qualifizierte elektronische Signatur auf den Chip des Ausweises nachgeladen werden.

5.9. Neue Formen bargeldlosen Bezahlens

Clubs in Barcelona und Amsterdam bieten eine neue Variante des bargeldlosen Bezahlens an. Die Gäste müssen sich dazu einen Chip in den Oberarm injizieren lassen. Ein Lesegerät registriert dann jeden Besuch und die konsumierten Speisen und Getränke. Angenehmer Nebeneffekt für die/den Clubbetreiber/-in ist die Bindung der Kundinnen/Kunden, denn mit dem RFID-Chip können sie nur dort bezahlen.

Absehbar ist, dass die Menge der in den Oberarm injizierten Chips begrenzt ist. Offen bleibt die Frage, ob sich mehrere Chips gegenseitig stören. Auch medizinische Probleme wie Entzündungen beim Einsetzen und Entfernen sind denkbar.

5.10. Sicher in Krankenhäusern

Auch in Krankenhäusern laufen erste Projekte an. Beispielsweise auf Neugeborenenstationen sollen RFID-Armbänder die Entführung von Babys verhindern. In psychiatrischen Bereichen schlagen die Armbänder automatisch Alarm, wenn Patienten unbefugt die Station verlassen. Außerdem sollen die auf den Chips befindlichen Daten über Medikamente und Therapien eine schnelle und zielgerichtete Behandlung unterstützen.

5.11. Leistung im Sport messen

Bei Sportlern lässt sich über mit RFID-Chips versehene Fuß- oder Armbänder die Geschwindigkeit sekundengenau messen. Läuft beispielsweise die Sportlerin oder der Sportler an einem Lesegerät vorbei, so erfasst es sie/ihn an diesem Punkt und misst die gelaufene Zeit.

5.12. Organisation der Abfallentsorgung

Auch für den Bereich der Abfallentsorgung bietet RFID neue Möglichkeiten. Mit RFID-Chips versehene Abfallcontainer ermöglichen eine eindeutige Zuordnung des Containers zu einem Haushalt oder auch zu einem Unternehmen. Zudem lassen sich Leergutdaten, wie zum Beispiel der Zeitpunkt oder die Häufigkeit der Leerung sowie das Gewicht der zu entsorgenden Abfallmenge leicht feststellen und übermitteln. Die Kosten der Entsorgung lassen sich damit nicht mehr nur pro Abfalltonne oder Container, sondern direkt nach Gewicht abrechnen.

5.13. Service an öffentlichen Plätzen

Auch Bibliotheken nutzen die RFID-Technologie. Mit RFID-Chip ausgestattete Bücher sollen den Ausleihvorgang beschleunigen. Zugleich bietet der Chip einen guten Diebstahlschutz. RFID verändert auch in Kantinen, beim Skifahren oder in Museen sowie in Schwimmbädern den Service. Wartezeiten verringern sich, manuelle Kontrollen entfallen; gleichzeitig verschwindet aber auch der persönliche Service.

RFID-Chips lassen sich in Plastikkarten integrieren, auf denen die Identifikationsnummer einer Person gespeichert ist. Das ermöglicht das personengebundene bargeldlose Zahlen ebenso wie das automatische Einstellen der Trainingsgeräte auf das Körpergewicht und die Größe einer/eines Trainierenden oder das automatische Öffnen von Schleusen.

5.14. Intelligente Haushaltsgeräte

Kühlschränke oder Waschmaschinen, die mitdenken, gibt es bisher nur als Prototypen. Der Kühlschrank scannt die enthaltenen Produkte und gleicht sie mit einer zuvor festgelegten Bestandsliste ab. Fällt etwa der Bestand an Milch unter die festgelegte Stückzahl, dann registriert der Kühlschrank das und setzt Milch auf die Einkaufsliste, vergleichbar mit einem Warenwirtschaftssystem. Diese Liste geht dann per Internet an den Einkaufsladen.

Betritt später die Kundin oder der Kunde den Laden und wird mittels Chipkarte (oder auch mittels eines implantierten Chips) identifiziert, so lässt sich auf einem Display der aktuelle Einkaufszettel aufrufen. Da sich das System Einkaufsverhalten merken kann, kann die Kundin oder der Kunde auch daran erinnert werden, welche Produkte sie/er üblicherweise noch kauft und die nicht vermerkt sind. Damit das funktioniert, müssen alle in dem Kühlschrank befindlichen Lebensmittel mit einem RFID-Chip versehen sein.

Theoretisch könnte der Kühlschrank auch gleich eine Warenbestellung initiieren, so dass die/der Kundin/Kunde nicht einmal mehr den Laden betreten muss. Die Ware ließe sich dann automatisch zu vorher festgelegten Zeiten anliefern und per Kontoeinzug oder Kreditkarte bezahlen. Ähnlich die Idee bei Waschmaschinen: Sie sollen erkennen, was sich in der Trommel befindet und dann das entsprechende Waschprogramm vorschlagen.

5.15. eGK: Die elektronische Gesundheitskarte der BRD

Rund 70 Millionen gesetzlich Krankenversicherte sollten vom 1. Januar 2006 an diese Chipkarte erhalten. Dies sieht das Gesetz zur Modernisierung der gesetzlichen Krankenversicherung in der BRD vor. 2006 wurde die elektronische Gesundheitskarte (eGK) in einigen Regionen verschiedener Bundesländer der BRD probeweise eingeführt (vgl. http://www.die-gesundheitskarte.de/testphase/testregionen/index.html). Die im Jahr 2007 durchgeführte Testphase wurde in einigen Ärztekammerbezirken gestoppt, da wesentliche technische und organisatorische Voraussetzungen weiterhin nicht geklärt sind.

Offenbar verschiebt sich die Einführung der elektronischen Gesundheitskarte erneut. Schon vor drei Jahren sollte die neue Karte kommen, allerdings konnten die mehreren geplanten Starttermine aufgrund diverser Schwierigkeiten mehrmals nicht gehalten werden. Zuletzt hieß es, dass die neuen Karten zur Speicherung von Patientendaten im Herbst 2008 in Teilen Deutschlands eingeführt werden sollten. Neuen Berichten zur Folge ist nun das Jahr 2009 als neuer Termin anvisiert.

Die elektronische Gesundheitskarte soll zukünftig persönliche Daten ihres Besitzers, Notfallinformationen, Arztdokumente und Rezepte für verordnete Arzneimittel enthalten. Dadurch sollen beispielsweise Überweisungen oder gedruckte Rezepte überflüssig werden. Der Patient soll beim Besuch der Apotheke seine Karte vorlegen können, von deren Speicherchip die Informationen über die verordneten Medikamente mit einem Lesegerät abgerufen werden können. Mit der Einführung der eGK wird das so genannte elektronische Rezept möglich. Das vom Arzt verordnete Medikament muss nicht mehr in Papierform an den Patienten ausgehändigt werden, sondern lässt sich direkt auf die eGK schreiben, speichern und in der Apotheke lesen. Weiterhin soll, vorerst auf freiwilliger Basis, die Karte auch der Bereitstellung medizinischer Daten dienen und zum Beispiel Informationen über eine Notfallversorgung oder eine Arzneimitteldokumentation bereithalten.

Damit die neue Gesundheitskarte überall lesbar ist, müssen Apotheken, Ärzte, Krankenhäuser sowie die Krankenkassen mit einer entsprechenden Software und sogenannten Terminals ausgestattet werden. Trotzdem sich das Gesundheitswesen von der Nutzung der Chipkarten deutliche Einsparungen erhofft, gibt es harsche Kritik von den Datenschützern. Die Datenschützer gehen davon aus, dass die sensiblen Informationen und Daten nicht genügend geschützt sind und somit ein etwaiger Datenmissbrauch für die Versicherten schwerwiegende Folgen nach sich ziehen könnte.

Datenschutz Gesundheitskarte

Es bestehen auch grundsätzliche datenschutzrechtliche Bedenken bezüglich der Übermittlung und Speicherung von höchstpersönlichen Daten im Internet. Zudem befürchten Kritiker, dass die Karte das Recht der Bürger auf informationelle Selbstbestimmung verletzt. Hierzu gibt es bereits Stimmen von Politikern und Spitzenmanagern der Krankenkassen, die das Freiwilligkeitsprinzip der Datenspeicherung auf der Gesundheitskarte verlassen wollen. Ärzte und Datenschützer warnen vor der Gefahr des „gläsernen Patienten". Nach ihrer Meinung soll der Patient der „Herr seiner Daten" sein und bleiben.

Das setzt voraus, dass er in die Lage versetzt wird, die über ihn gespeicherten Daten einsehen zu können. Dafür ist im häuslichen Bereich ein spezielles Lesegerät notwendig, auch muss bei der gewünschten Serverlösung ein Weg eröffnet werden, dem Patienten Zugriff auf seine dort gespeicherten verschlüsselten Daten zu ermöglichen. In Arztpraxen und Apotheken sollen sogenannte Kiosksysteme eingerichtet werden, über die Patienten auf ihre Daten zugreifen können.

Inzwischen geht man in der Diskussion so weit, dass künftig Patienten ihre Krankheitsdaten, Verschreibungen usw. selbstständig löschen können und dürfen, was aber wiederum die zielgerichtete Behandlung durch den Arzt erheblich einschränkt. Eine „geschönte" oder unvollständige Patientenakte wiederum nutzt dem Arzt nichts und ist u. U. sogar gefährlich.

5.16. ELENA – Die Job-Card der BRD mit dem Namen einer griechische Göttin

Rund 40 Millionen deutsche ArbeitnehmerInnen sollen bald ELENA kennen lernen und die JobCard erhalten - und Unternehmen dadurch jährlich 500 Millionen Euro an Verwaltungskosten einsparen. Doch Datenschützer warnen vor dem »gläsernen Arbeitnehmer«, denn für das JobCard-Verfahren sollen die monatlichen Gehälter und Einkommen in einem bundesweiten Beschäftigtenverzeichnis gespeichert werden.

Das Bundeskabinett der BRD hat den Gesetzentwurf zu ELENA beschlossen. Zum 1.1.2012 soll der elektronische Entgeltnachweis kommen, der bei der Beantragung von Sozialleistungen wie dem Arbeitslosengeld I, dem Erziehungsgeld und dem Wohngeld eingeführt wird. Das Elena-Verfahren (elektronischer Entgeltnachweis) ist ein vorgesehenes Verfahren, mit dem Einkommensnachweise elektronisch mit Hilfe einer Chipkarte mit integriertem Zertifikat zur Erstellung qualifizierter elektronischer Signaturen erbracht werden sollen.

Geplant war und ist, dass eine beliebige, nach einheitlichem Standard (SASCIA, eCard-API) funktionierende Chipkarte (EC-/Maestro-Card, eGK, ePA etc.) verwendet werden kann. Der Begriff wird auch verallgemeinernd für das gesamte JobCard-Verfahren gebraucht, nämlich für die geplante zentrale Speicherung von Arbeitnehmerdaten und die Nutzung dieser Daten durch die Agenturen für Arbeit und weitere Stellen.

Der Begriff JobCard ist in der Kommunikation mittlerweile durch die Formulierung Elena - für »elektronischer Entgeltnachweis« (ELENA-Verfahren) - ersetzt worden (zwischenzeitlich war auch vom elektronischen Einkommensnachweis die Rede). Elena kennzeichnet ein Verfahren, welches die Chipkarte von Drittanbietern, die über die Zertifikatsidentitätsnummer dem Teilnehmer zugeordnet wird, als Schlüssel verwenden soll.

Sicherheitshalber soll jede/-r Beschäftigte eine Chipkarte mit einer qualifizierten Signatur erhalten. Die Job-Card soll den Zugriff auf sämtliche Daten des Beschäftigungsverhältnisses ermöglichen, also die Beschäftigungszeiten, die Höhe des Gehalts und Einkommens sowie die Kündigung. Das soll die Verwaltungsabläufe der Arbeitsämter und Jobcenter beschleunigen, so dass die Bearbeitung und Genehmigung von Lohnersatzleistungen schneller erfolgen kann.

Den Firmen bleiben die Kosten für Arbeitsbescheinigungen etc. erspart. Die Regierung beziffert das Einsparpotenzial insgesamt auf 500 Millionen Euro pro Jahr für die Unternehmen. Rund 60 Millionen Bescheinigungen in Papierform stellen Unternehmen jährlich aus. Elektronische Meldeverfahren sollen die Papierflut künftig eindämmen und Kosten sparen. Datenschützer warnen vor der zentralen Speicherung dieser sensiblen Daten.

Ersparnis für Bürokratie

Der elektronische Einkommensnachweis (ELENA), früher auch Jobcard genannt, soll ab 2011 auch die die Arbeit in deutschen Amtsstuben und Arbeitsagenturen erleichtern. Die schnelle Online-Abfrage der auf einem Zentralrechner der Rentenversicherung gespeicherten Einkommensnachweise soll helfen, mehr als 100 Millionen Euro Bürokratiekosten pro Jahr zu sparen. Die Kosten für die notwendigen Signaturkarten von 10 bis 45 Euro pro Jahr, die von den Arbeitnehmern getragen werden müssen, sollen für die Bezieher von Arbeitslosengeld II von den Arbeitsagenturen übernommen werden. Nach etlichen Verzögerungen und unbeschadet der Bedenken von Datenschützern soll das ELENA-Verfahren vor allem dadurch beschleunigt umgesetzt werden, dass es für die Vorgänge der Bundesagentur für Arbeit als Pflichtverfahren definiert wird.

Kosten tragen die ArbeitnehmerInnen

Dafür kommen Kosten auf die ArbeitnehmerInnen zu. Sie müssen sich eine qualifizierte digitale Signatur besorgen, die auf dem kommenden elektronischen Personalausweis oder »auf jeder modernen Bankkarte« gespeichert wird. Derzeit kostet eine solche Signatur mit einem drei Jahre gültigen Zertifikat bei den Trustcentern durchschnittlich 60 Euro. Bis zum Start von ELENA hofft man, dass die Kosten auf 40 Euro gefallen sind.

Die deutsche Bundesregierung jedoch sieht ELENA als Antriebsmotor, der der seit mehr als 10 Jahren angeboten Signaturtechnik den nötigen Anschwung verleiht.

Von der Signaturkarte zur Jobkarte

Derzeit erstellen 2,8 Millionen deutsche Arbeitgeber jährlich ca. 60 Millionen Bescheinigungen, die aus dem EDV-System auf Papiervordrucke der Bundesanstalt für Arbeit gedruckt werden, um anschließend in andere Systeme eingegeben zu werden. ELENA soll diesen Medienbruch beseitigen: Arbeitgeber senden ihre Entgelt-Daten an eine Zentrale Speicherstelle (ZSS), wo sie von Sachbearbeitern der Bundesanstalt für Arbeit abgefragt werden können, sowie der Arbeitnehmer mit seiner qualifizierten digitalen Signatur die Einwilligung zur Datenabfrage dokumentiert hat.

Dabei ist ELENA selbst keine eigenständige Chipkarte, sondern nur eine auf einer Karte aufgebrachte qualifizierte Signatur, die öffentlich überprüft werden kann und die manuelle Unterschrift eines Antragsstellers auf Leistungszahlungen ersetzt. Gleichzeitig soll sie die »rechtssichere Kontrolle des Datenabrufs« feststellen.

Die Regierung der Bundesrepublik Deutschland will für die JobCard allerdings keine eigene Infrastruktur aufbauen, sondern auf vorhandene Strukturen zurückgreifen. Das heißt, dass das JobCard-Verfahren auf einer Signaturkarte basieren kann, wie sie die Banken künftig herausgeben wollen. Auf der Karte selbst sind keine Verfahrensinformationen enthalten, sondern sie dient lediglich als Schlüssel, um die nötigen Informationen, die zentral gespeichert sind, freizuschalten. Um eine JobCard zu erhalten, muss jeder Arbeitnehmer einen Antrag bei einer Registrierungsstelle einreichen und sich dabei durch persönliches Erscheinen legitimieren.

Dazu will die Bundesregierung in Deutschland flächendeckend Registrierungsstellen einrichten, die beispielsweise in Bankfilialen untergebracht werden könnten. Für eine Teilnahme am JobCard-Verfahren stellt eine zentrale Stelle namens „Registratur Fachverfahren“ eine Verknüpfung zwischen der Identitätsnummer auf der JobCard und der Sozialversicherungsnummer her. Nach demselben Zuordnungsprinzip könnte übrigens aus der Kombination der Karten-ID-Nummer mit der Steuernummer auch eine Elster-Card (elektronische Steuererklärung) entstehen oder aus der Verknüpfung ID-Nummer und der vom Einwohnermeldeamt vergebenen Nummer eine Bürgerkarte.

Beim elektronischen Einkommensnachweis wird für die Datenabfrage eine digitale Signatur benötigt. Mit ihr dokumentiert der Arbeitnehmer sein Einverständnis, dass sich die Behörde Nachweise über seine Beschäftigungszeiten und Einkommensverhältnisse auf elektronischem Wege besorgt. Grundsätzlich ist es nicht notwendig, dass für ELENA eine eigene Karte erstellt wird. So können der kommende elektronische Personalausweis oder die Gesundheitskarte und etliche Bankkarten mit Zertifikaten für die elektronische Signatur ausgestattet werden, die dann bei ELENA benutzt werden. Während die Einrichtung und Nutzung einer digitalen Signatur vom Bürger bezahlt werden muss, haben die Arbeitgeber den größten Nutzen von der geplanten Neuregelung: 6,5 Millionen Beschäftigungsnachweise werden jährlich allein zur Vorlage bei den Arbeitsagenturen ausgedruckt und verschickt.

Datenschutz

Mit ELENA wird nicht der schönen griechischen Göttin gehuldigt, sondern eine hässliche, datenschutzwidrige Großdatenbank in die Welt gesetzt, heißt es in der Stellungnahme des Datenschützers Thilo Weichert, dem Leiter des unabhängigen Landeszentrums für Datenschutz in Schleswig-Holstein. Weichert kritisiert die Speicherung auf Vorrat, die nicht allein beim Beantragen von Sozialleistungen genutzt werden könnte. Auch andere Behörden, allen voran die Finanzämter, könnten sich für die Datensammlung interessieren, wenn sie einmal in der Welt ist. Kritisch sei dabei der Datenzugriff ohne Kenntniss der Betroffenen. Sind Daten einmal vorhanden, sind diese schnell vielfältigen Begehrlichkeiten ausgesetzt, gegen die die Betroffenen keine Abwehrmöglichkeiten haben.

5.17. Die Medaille hat zwei Seiten

Die Vorstellung ist verlockend, dass die Waschmaschine, wenn der teure und RFID-etikettierte Kaschmirpullover in der Waschmaschine verschwindet, Meldung macht, dass es nun ganz und gar ungeschickt wäre, dieses gute Stück zu kochen.

Auch viele Tierbesitzer haben ihr Haustier gechippt, in der Hoffnung, dass böse Hunde- und Katzenschänder von der Malträtierung ihres Lieblings absehen und dass es – lebendig oder tot – eindeutig nach einem Verschwinden identifiziert werden kann. Sicherheitstechnisch interessant dürften die Reifen sein, die im Kraftfahrzeug darauf hinweisen, dass der Luftdruck hinten links abfällt. Ein Auto, das in der Lage ist, mit den Reifen zu kommunizieren, ist verlockend.

Die RFID-etikettierten WM-Fussballkarten haben zwar im Vorfeld für viel Ärger gesorgt, allerdings mehr wegen des Vergabeverfahrens als wegen der Chips. Zu Recht haben aber auch manche gefragt, weshalb diese vielen persönlichen Angaben gemacht werden müssen, um ein Fußballspiel sehen zu können.

Auch die elektronische Gesundheitskarte hat Vor- und Nachteile. Kritiker fürchten jedoch, dass die Karte zu viele höchstpersönliche Gesundheitsdaten enthält; sie sehen dadurch das Persönlichkeitsrecht auf Datenschutz in Gefahr.

Die einen finden es äußerst praktisch, mit dem eingespritzten Chip im Oberarm in der Disco zu bezahlen, für die anderen ist die Vorstellung uferloser Kontrolle unerträglich.

Die meisten Kundinnen/Kunden würden vermutlich nicht wollen, dass ihr Einkaufsverhalten bis ins letzte Detail nachvollziehbar bleibt – sie fänden es wahrscheinlich aber praktisch, beim Einkauf im volltechnisierten Supermarkt darauf hingewiesen zu werden, dass bislang einige der üblicherweise gekauften Lebensmittel noch nicht im vollelektronischen Einkaufswagen liegen und welche dieses sind. Letztlich laufen Kundinnen/Kunden Gefahr, dass ihr gesamtes Kaufverhalten ausspioniert wird. Einmal angenommen, der intelligente Kühlschrank sei serienreif und funkt den Einkaufszettel vorab schon mal in den Supermarkt. Die Unternehmen können sich dann gezielt auf die/den Kundin/Kunden vorbereiten. Bereits durch das digitale Abkassieren lässt sich nicht nur das Kaufverhalten, sondern auch das Kaufpotenzial der Verbraucher/-innen analysieren.

Die Animation zum Kauf erfolgt dann gezielt auf die/den Kundin/Kunden zugeschnitten. Vielschichtig dürften die Reaktionen der Kundinnen/Kunden sein, wenn sie ihre Einkäufe in einem fast personalfreien Geschäft zu tätigen hätten. Solange die Info-Terminals alle Angaben liefern, die für einen Einkauf erforderlich sind, ist der Unterschied kaum bemerkbar, aber jeder brauchte schon mal weitergehende Hilfe durch eine/-n Verkäufer/-in.

Wichtig ist es, die Verbraucher/-innen über den Einsatz von RFID zu informieren:

- Welche Daten werden zu welchem Zweck gespeichert, werden die Daten weiter gegeben und wenn ja, an wen?
- Wie lange werden sie aufbewahrt und welche Verknüpfungen der Daten mit ggf. weiteren Daten der Kundinnen/Kunden werden vorgenommen.
- Welche werbestrategischen Maßnahmen werden aufgrund des Datenmaterials eingeleitet?

RFID und weitere Selbstbedienungstechniken mögen aus der Sicht mancher Verbraucher/-innen ein Teil einer schönen neuen Welt sein. Es gab aber auch eine Zeit, da beriet und bediente uns ein/-e Verkäufer/-in an der Käsetheke, da verkaufte uns jemand am Schalter eine Fahrkarte und den Dauerauftrag mit der persönlichen Unterschrift nahm am Bankschalter ein/-e Angestellte/-r entgegen. Heute wählen wir fertig abgepackten Käse aus der Kühltruhe, schlagen uns mit Fahrkartenautomaten herum und erledigen Bankgeschäfte online zu Hause.

Im Handel führen diese Trends dazu, dass der beratungsintensive Einzelhandel, wie zum Beispiel Warenhäuser in den Innenstädten oder kleine Fach-Einzelhandelsgeschäfte Marktanteile verlieren, die Beschäftigung bei gleichzeitigem Verlust der Servicequalität rückläufig ist und dass letztendlich diese Unternehmen schließen. Gewinner des Verdrängungs- und Preiswettbewerbs sind die großen Discount-Unternehmen an der Peripherie der Städte.

5.18. Bei bester Gesundheit

Auch über die Frage der gesundheitlichen Belastungen/Gefahren herrscht Uneinigkeit. Auffällig ist, dass es einerseits offiziell heißt, alles sei harmlos, sich aber andererseits bestimmte Personengruppen schützen sollen. Die Diskussion über mögliche gesundheitliche Folgen ist nicht neu; sie entstand erstmals vor mehr als 50 Jahren, als Radiogeräte flächendeckende Verbreitung erlangten. Weitere Technologien, die ebenfalls elektromagnetische Wellen erzeugen, kamen hinzu: Mobiltelefone (Handys), schnurlose Telefone, drahtlose Nahbereichsfunknetze (Wireless Local Area Network – WLAN), elektronische Warensicherheitssysteme.

Träger/-innen von Herzschrittmachern, Infusionspumpen oder metallischen Implantaten etc. sollen sich bei der behan- delnden Ärztin oder beim behandelnden Arzt darüber informieren, ob bei ihrem Gerät eine Beeinflussung durch Warensicherungsanlagen möglich ist.

RFID-Systeme nach dem Standard von „EPCGlobal" funken an die Schreib-/Lesegeräte im selben Frequenzbereich wie Mobiltelefone; die in Europa maximal erlaubte Sendeleistung liegt für beide Systeme bei zwei Watt. Aufgrund dieser Parallelen erscheint eine Übertragung der Untersuchungsergebnisse des Mobilfunks auf die RFID-Technologie zulässig.

Die meisten Studien kommen zu dem Ergebnis, dass keine Gesundheitsschädigungen zu befürchten seien, da geltende Grenzwerte eingehalten würden. Grenzwerte sind jedoch keine fixe Größe; sie beruhen auf Erfahrungen, Messwerten, Schätzungen etc. und sind abhängig von Rahmenbedingungen. (weitere Informationen unter www.elektrosmog.com).

Die gesundheitlichen Folgen eines Wellensalats mit gleichzeitig auf den Menschen treffenden unterschiedlichen Wellenquellen sind in den Grenzwerten ebenfalls nicht berücksichtigt. Schlafforscher der Universität Zürich haben nachgewiesen, dass sich die Hirnströme schlafender Menschen durch Handys verändern. Ob daraus weitere Folgen für die Gesundheit resultieren können, ist derzeit noch unklar. Menschen mit Herzschrittmachern, Insulinpumpen und anderen elektrisch betriebenen Implantaten sollen nach derzeitigem Erkenntnisstand mindestens 25 Zentimeter Abstand zu Mobiltelefonen halten. Wer ein Hörgerät trägt, muss in der Nähe von schnurlosen Telefonen (bis 30 cm Abstand) und Handys (bis 70 cm Abstand) mit Brummgeräuschen rechnen. Beschäftigten mit elektrisch betriebenen Implantaten ist daher dringend anzuraten, sich nicht in der unmittelbaren Nähe der Sende- und Empfangsgeräte für RFID-Chips aufzuhalten.

Die Erkenntnisse des Bundesamts für Strahlenschutz in der BRD bestätigen einen laxen Umgang mit der neuen Technik: Messungen in Kaufhäusern, im Bereich von Warensicherungsanlagen mit RFID-Technik (dort eingeführt zum Schutz vor Diebstahl), ergaben im Bereich niederfrequenter Felder und im Kurzwellenbereich zeitweise zu hohe Werte.

Die Messungen wiesen Pulsspitzen mit einer magnetischen Flussdichte aus, die über den für die allgemeine Bevölkerung empfohlenen Referenzgrenzwerten der „International Commission on Non-Ionizing Radiation Protection" (ICNIRP) liegen.

Pauschal gilt:

- Je größer der erforderliche Leseabstand desto höher die Frequenz.
- Je höher die Frequenz desto stärker das elektromagnetische Feld.
- Je stärker das elektromagnetische Feld desto höher die Gefahr einer gesundheitlichen Belastung.
- Passive Transponder funken nur dann, wenn eine Leseeinrichtung sie erreicht.
- Aktive Transponder funken immer und stellen somit potenziell eine Dauerbelastung dar.

5.19. Hemmnisse der RFID-Technik

Während der momentan noch stattfindenden Erprobungsphase liegt der Schwerpunkt im Taggen von Paletten und Gebinden, um die Warenzusammenstellung, den Warenein- und -ausgang sowie den weiteren Verbleib transparenter zu machen. Vollautomatische „Future Stores" als „Standardgeschäft" sind noch Visionen.

(1) Ein verbindlicher Einheitsstandard fehlt
Die Idee, jedes einzelne Produkt mit einem weltweit kompatiblen Chip zu versehen, ist noch Zukunftsmusik. Derzeit gibt es zwar einzelne Feldversuche, diese sind aber bisher auf zweiseitige und nicht auf beliebige Geschäftskontakte beschränkt. Ein globaler Einheitsstandard befindet sich derzeit noch in der Entwicklungsphase.

(2) Die Technologie für den RFID-Einsatz ist nicht perfekt
Flüssigkeiten und metallische Oberflächen wie zum Beispiel Alu-Folie bereiten momentan noch technische Probleme beim Auslesen der Daten auf den RFID-Chips. Weiterhin ungeklärt ist die Frage, wie sich die auf dem RFID-Chip ausgelesenen Daten sicher vor Manipulationen auf das Lesegerät übertragen lassen.

(3) Das Taggen von Einzelprodukten ist teuer
Jedes einzelne Produkt benötigt einen Chip; das betrifft nicht nur teure Produkte, bei denen die Kosten einen vertretbaren Kostenanteil ausmachen, sondern auch Produkte, die nur einige Cents kosten. Hier bleibt die Entwicklung der Polymertechnik abzuwarten. Mit dieser Technik könnte es gelingen, RFID-Chips zu rentablen Konditionen für alle Produkte zu drucken. Die Notwendigkeit, alle Waren mit Chips auszustatten, ist und bleibt die Voraussetzung dafür, dass Informationen zu jedem einzelnen Produkt gelangen und sich die Waren an der Kasse ohne Kassierer/-in im Pulk erfassen lassen.

(4) Virengefahr
In RFID-Chips eingeschleuste Viren könnten bewirken, dass sich Lagerbestände und die Bestände in den Läden nicht mehr zuverlässig abfragen und auffüllen lassen und, dass die Logistikkette außer Kontrolle gerät. Zum Beispiel wäre es so möglich, Waren zu bestellen und in falsche Geschäfte zu liefern.

„RFID wird einen einschneidenden Einfluss auf jeden Bereich der

Zivilisation haben, ungefähr so wie die Druckerpresse, die industrielle Revolution und das Internet und die Computer die Gesellschaft verändert haben. ... RFID ist ein ganz großes Ding. Ihr Einfluss wird umfassend, persönlich und tiefgreifend sein. Das ist die größte Erfindung, seit Edison uns die Glühbirne geschenkt hat." Rick Duris, Frontline Solutions Magazine, Dezember 2003

Datenschutz

Datenschützer kritisieren diese Technologie, mit denen der Handel langfristig den Barcode ablösen will. Im Februar 2004 hatte der »Future Store« des Handelskonzerns „Metro" in Rheinberg Kundenkarten mit RFID zurückgezogen, nachdem Datenschutzaktivisten des Vereins „FoeBuD" diese entdeckt und kritisiert hatten. Dafür wurde Metro in der BRD mit dem Big Brother Award ausgezeichnet. Vereine wie „quintessenz", „vibe.at in Österreich FoeBUD „ in der BRD vergeben einmal im Jahr den an George Orwells Vision „1984" angelehnten Negativpreis „Big Brother Award". Mit Hilfe der RFID-Technik lassen sich personenbezogene Daten verarbeiten und Rückschlüsse auf Personen ziehen. Das birgt sehr wohl datenschutzrechtliche Gefahren.

Wichtig wäre:
- Eine Kennzeichnungspflicht für Produkte mit Chip, das Recht, die darin gespeicherten Informationen einsehen zu können und den Chip nach dem Kauf permanent deaktivieren zu lassen.
- Firmen müssten ihre Kunden darüber informieren, wenn Sie Chips in Produkte integrieren – Nicht erst dann, wenn Sie persönliche Daten damit verknüpfen.
- Regelungen für Dritte, die den Chip auslesen könnten.

6. HANDLUNGSSPIELRÄUME FÜR BETRIEBSRÄTINNEN

6.1. Persönlichkeitsrechte in Gefahr

Auch und vor allem in der Arbeitswelt besteht die Möglichkeit, Leistungs- und Verhaltensprofile ohne Wissen oder Einverständnis der Mitarbeiter/-innen zu erstellen. In Verbindung mit Informationen aus anderen Datenbanken (Personaldaten, Zeiterfassungsdaten etc.) oder geografischen Ortungssystemen (zB GPS-Daten) können RFID-Techniken zu einer allumfassenden Datenverarbeitung und somit zu einer allgegenwärtigen Überwachung aller Personen führen. Bedenklich ist insbesondere die Möglichkeit der Unternehmen, mittels RFID in die Privatsphäre der Beschäftigten einzudringen. Das Nutzungspotenzial umfasst die verdeckte Sammlung einer Vielzahl von Daten, die zum Beispiel Auskunft darüber geben, welche Kleider eine bestimmte Person trägt und welche Accessoires sie benutzt. Exakt erfassen lässt sich auch, was die Person am Arbeitsplatz (nicht) leistet und wie sie sich in bestimmten Situationen verhält.

Zutrittskontroll- oder Zeiterfassungssysteme ermöglichen darüber hinaus, Personen unbemerkt flächendeckend zu überwachen und Bewegungsprofile zu erstellen. Das Auslesen von Ausweisen ist auch außerhalb des Unternehmens möglich. Wenn personenbezogene Daten unmittelbar auf RFID-Tags gespeichert oder in Datenbanken verknüpft werden (zB Zeiterfassung, Bewegungsdaten, Kantinenabrechnung, Produktvorlieben bei Essen, Kleidung etc.), dann ist dies ein Eingriff in die Persönlichkeitsrechte. RFID eröffnet durch kontaktloses Erfassen – also ohne Zutun des Beschäftigten – eine neue Qualität der Überwachung. Die Technik ermöglicht ein zeitlich und räumlich allgegenwärtiges Bespitzeln der Menschen. Es gibt zwar Schutzmaßnahmen, um die Gefahren des RFID-Einsatzes zu begrenzen. Es gibt allerdings kein spezielles RFID-Gesetz oder ein Arbeitnehmer/-innen-Datenschutzgesetz.

6.2. Rechte der Beschäftigten im Arbeitsverhältnis

Durch die neuen Möglichkeiten der Datenvernetzung und -speicherung besteht die Gefahr, dass Rechte verletzt werden, insbesondere das allgemeine Persönlichkeitsrecht sowie das Recht auf informationelle Selbstbestimmung.

- Entsprechend den Informationspflichten des Arbeitgebers haben die Beschäftigten das Recht auf Auskunft über die gespeicherten persönlichen Daten.
- Zudem haben die Beschäftigten Korrekturrechte. Unrichtig gespeicherte personenbezogene
- Daten sind zu berichtigen, insbesondere wenn die Speicherung unzulässig erfolgt ist.
- Betroffene haben grundsätzlich ein Widerspruchsrecht.
- Ein wichtiger Grundsatz im Datenschutz ist das Prinzip der Datenvermeidung und Datensparsamkeit. Gestaltung und Auswahl von Datenverarbeitungssystemen sollten sich an dem Ziel ausrichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen.
- Wenn Daten erhoben werden, dann grundsätzlich beim Betroffenen
- Ein weiterer Grundsatz ist die Pflicht zur Transparenz bei der Datenerhebung. Der Arbeitgeber hat als verantwortliche Stelle entsprechende Informationspflichten. Danach ist die/der Betroffene darüber zu unterrichten, wer für die Datenerhebung verantwortlich ist, zu welchem Zweck die Daten erhoben werden und wohin sie gehen.
- Daten dürfen außerdem nur für den Zweck verwendet werden, für den sie ursprünglich erhoben worden sind.

6.3. Betriebe wandeln sich

IT-Systeme durchdringen alle betrieblichen Bereiche; die neue RFID-Technologie ebenso. Damit verknüpfte IT-Systeme rationalisieren und vereinfachen nicht nur das Warenwirtschaftssystem, sie sind vielmehr auch ein umfassendes Dokumentations-, Registrier-, Verarbeitungs- und Auswertungs- sowie Kontroll-Werkzeug. Zusätzlich ermöglichen sie als zentraler technischer Bestandteil die überbetriebliche Vernetzung von Daten über Produkte und ihre Qualitäten, über das logistische System, die Arbeitnehmer/-innen und ihr Leistungsvermögen sowie die Kundinnen/Kunden und nicht zuletzt ihre Eigenschaften wie Einkaufsverhalten, Vorlieben, Alter, Geschlecht etc. Durch die zentrale Stellung von IT-Systemen im Betrieb bekommt der Datenschutz eine neue, oft unterschätzte Dimension. Auch ist zu bedenken, dass die Einführung und Weiterentwicklung von IT-Systemen nicht in erster Linie ein technischer Vorgang ist:

Komplexe IT-Systeme erreichen die Dimension einer Betriebsänderung, da sie umfassend in die betrieblichen Abläufe und Strukturen eingreifen. Wirksamkeit und Effektivität von IT-Systemen hängen vom jeweiligen Betrieb ab. Vorhandene organisatorische Unzulänglichkeiten wirken sich demzufolge auch auf das IT-System aus. Kauft der Betrieb vorgegebene, fremde Organisationsmodelle mit IT-Standardlösungen ein, dann ersetzen diese die bisherigen selbst entwickelten Strukturen. Gerade bei neuen Technologien wie der RFID-Technik können führende Unternehmen Standards setzen, die sich dann auf die Organisation anderer Unternehmen auswirken – die IT-Lösung ist dann der Träger für solche Veränderungen.

RFID-Technologie verändert bereits jetzt die bisherigen betrieblichen Organisationsformen und dies hat Auswirkungen auf jeden einzelnen Arbeitsplatz. RFID-Technologien sind ein mächtiges Instrument der Kontrolle von Leistung und Verhalten der Beschäftigten. Daraus folgt: Schutz- und Gestaltungsansprüche sind aufgrund ständiger betrieblicher Veränderungen durch die Weiterentwicklung und laufende Verbesserung dieser neuen Technologie und der entsprechenden IT-Systeme nicht mehr abschließend und auf Dauer regelbar. Benötigt wird daher ein neuer Typ entwicklungsfähiger Mitbestimmungsregelungen mit begleitenden Informations- und Analyseprozessen.

Technik im Handel ist notwendig und erforderlich, um die Prozesse in der Warenwirtschaft, der Lieferkette und an der Schnittstelle zur/zum Kundin/Kunden in einer globalisierten Welt zu steuern. Doch wenn eine starke Technikzentriertheit bis hin zur Technikfaszination überwiegt, dann sind die Menschen im Arbeitsprozess in Gefahr, allenfalls als Restgröße und Einsparpotenzial betrachtet und behandelt zu werden.

6.4. Der globalisierte Handel

Technikeinsatz im Handel an der Schnittstelle zur/zum Kundin/Kunden verlagert Aufgaben der Angestellten in den Bereich der Selbstbedienung. In der Erprobungsphase haben die Verbraucher/-innen meist noch Wahlmöglichkeiten zwischen der herkömmlichen Art und Weise der Inanspruchnahme von Dienstleistungen und der technikunterstützten Selbstbedienungsform. Doch dabei bleibt es nicht. Etablierte Verfahren werden Schritt für Schritt abgebaut und am Ende eingestellt.

Ein Beispiel:

Wenn es an der Käsetheke nur noch drei Sorten Käse gibt, während im Regal daneben hundert abgepackte Sorten zur Auswahl stehen, schwinden nach und nach die Kunden; die/der Verkäufer/-in macht nebenher andere Arbeiten und ist dann immer seltener an der Käsetheke anzutreffen, was die letzten Kundinnen/Kunden vergrault. Die Theke wird geschlossen und die/der Verkäufer/-in dort nicht mehr benötigt.

Seit Mitte der 90iger Jahre kämpfen die Unternehmen im Ringen um Marktanteile mit immer härteren Bandagen. Die Expansion der Verkaufsflächen bei stagnierenden Umsätzen, die Ausdehnung der Ladenöffnungszeiten und eine aggressive Preispolitik haben den Konkurrenzkampf und Verdrängungswettbewerb im Einzelhandel beschleunigt. Auch in Teilbranchen des Großhandels hat seit einiger Zeit ein Verdrängungswettbewerb begonnen, der Arbeitsplätze vernichtet.

Ein forcierter Technikeinsatz, zum Beispiel RFID zur Optimierung der logistischen Prozesse oder direkt im Verkauf (Selbstzahlerkassen, Info-Terminals, elektronische Regalauszeichnung etc.) wird bisherige Arbeitsprozesse automatisieren und einen geringeren Arbeitskräfteeinsatz im Lager, Fuhrpark oder im Verkauf ermöglichen. Mittel- und langfristig reduzieren sich damit die Beschäftigungschancen im Handel noch weiter.

Die vom Handel selbst initiierten Rabattschlachten und die „Geiz-ist-geil"-Mentalität der Unternehmen bleiben bei den Kundinnen/Kunden nicht ohne Wirkung. Je weniger Dienstleistung die/der Kundin/Kunde beim Kauf einer Ware geboten bekommt, desto weniger ist sie/er bereit, Preise zu bezahlen, mit denen noch qualifizierte Beratung, ausreichendes Personal und faire Arbeitsbedingungen möglich sind.

Technikeinsatz geht damit einher, dass Überwachungspotenziale steigen. Damit die Unternehmen keine Persönlichkeitsrechte missachten, braucht es einen Betriebsrat.

Betroffen sind die Menschen als Verbraucher/-innen und als Arbeitnehmer/-innen. Für die Beschäftigten können die Wirkungen weitreichend sein. Zeitabläufe werden transparent, Leistungsvergleiche sind jetzt auch außerhalb der Fließbandarbeit leicht möglich, Bewegungsprofile ebenso. Die Anforderungen steigen, nur die Besten bleiben. Wer nicht mehr mithalten kann, wird ersetzt. Obwohl die Unternehmen die Überwachungspotenziale bisher nicht ausschöpften, sind Betriebsräte trotzdem bereits mit Fällen konfrontiert, in denen Persönlichkeitsrechte von Beschäftigten missachtet wurden.

Seit dem Siegeszug der Handys sind drahtlose Verbindungen Alltag.

- Unklar ist, welche Folgen die Funktechnik und die zukünftig allgegenwärtige RFID-Technik für den menschlichen Organismus haben. Sind Auswirkungen auf unsere Gesundheit zu erwarten, wenn wir in einem Umfeld leben, das zahllose Gegenstände beherbergt, die unablässig Funkwellen aussenden?

- Was bedeutet es für die Umwelt, wenn der Abfall mit kleinsten Elektronikkomponenten durchsetzt ist, die im Recycling oder bei der Verbrennung Probleme bereiten?

- Wie wird sich unsere Energiebilanz verändern, wenn wir uns für die Organisation unseres Alltags mehr und mehr auf elektronisch hochgerüstete Utensilien verlassen, die auf Energie und eine dauerhaft betriebene Netzwerk-Infrastruktur angewiesen sind.

6.5. Es liegt in der Hand des Betriebsrats

Der Einsatz der RFID-Technologie bewirkt eine grundlegende Umgestaltung der Arbeitsabläufe und der Organisation im Handel; er macht Warenflüsse transparent und die dazugehörigen Daten für alle Beteiligten jederzeit verfügbar. So sind Betriebsräte oft auch mit negativen Folgen des RFID-Einsatzes konfrontiert, wie der Rationalisierung und Arbeitsverdichtung mit der Folge von Entlassungen sowie einer verstärkten Kontrolle der Beschäftigten und müssen im Rahmen der Mitbestimmungsmöglichkeiten Schutzrechte zugunsten der Beschäftigten einfordern und durchsetzen.

Um diese Aufgaben zu erfüllen sind Informationen beim Arbeitgeber anzufragen:

Welche Maßnahmen wurden bereits eingeleitet, welche sollen erfolgen, wie viele Beschäftigte sind in welcher Form betroffen?

(1) Das liegt in der Hand der Betriebsräte:

- Beschäftigte einbeziehen
- Bestandsaufnahmen machen
- Sachverständige hinzuziehen.

(2) Im nächsten Schritt ist es ratsam, im Gremium folgende Fragen zu erarbeiten:

- Welche Ziele hat der Betriebsrat?
- Welche Ziele haben die Arbeitnehmer/-innen?
- Was ist der beste Schutz für die Beteiligten?
- Welche Ziele sollten nach der Einführung des IT-Systems erreicht werden?
- Was spricht gegen die Ziele, was könnte die Erreichung der Ziele erschweren?
- Wie geht der Betriebsrat mit Einwänden um?
- Welche Ziele haben Priorität?

(3) Daraus folgt für die weitere Betriebsratsarbeit:
- Konkrete Einzelziele festlegen
- Forderungen aufstellen
- Erforderliche Beschlüsse fassen
- Rechte des Betriebsrats (Informationsrechte, Beratungsrechte, Kontrollrechte sowie Mitbestimmungsrechte) wahren und durchsetzen.

Unternehmer/-innen sind bestrebt, Gewinne zu maximieren. Sie begründen das Streichen von Arbeitsplätzen mit steigenden Kosten (z.B. durch die Investition in die RFID-Technik!) sowie einer unsicheren Marktposition und den damit verbundenen notwendigen Umstrukturierungen. Der spätere Profit liegt dann beim Unternehmen.

Betriebsräte sollten daher bereits vor (!) der Umstrukturierung mit Blick auf die zu erwartenden Verbesserungen ihre Ansprüche stellen. Dies können Forderungen nach mehr Qualifizierung (Weiterbildung der Mitarbeiter/-innen) sein, es können aber auch Ansprüche auf mehr Personal in der Beratung und Betreuung der Kundinnen/Kunden sein. Die Ansprüche der Beschäftigten sollten daran orientieren, welche Vorteile die Unternehmen durch den Einsatz von RFID erzielen. Handelt der Arbeitgeber in den hier genannten Fällen einseitig ohne Zustimmung des Betriebsrats, so ist das rechtswidrig. Hat der Arbeitgeber trotzdem eine mitbestimmungspflichtige Maßnahme im Alleingang durchgeführt, dann kann der Betriebsrat darauf drängen, dass sie rückgängig zu machen ist.

6.6. Personaldaten

Der Betriebsrat hat ein Mitbestimmungsrecht bei der Einführung und Anwendung von technischen Einrichtungen, die dazu geeignet sind, Verhalten und Leistung der Arbeitnehmer/-innen zu überwachen. Dieses Recht besteht unabhängig davon, ob die Maßnahme ausschließlich oder unter anderem auch darauf abzielt, die Arbeitnehmer/-innen zu überwachen. Auch ist es gleichgültig, ob beabsichtigt ist, aus den Aufzeichnungen Schlüsse über Verhalten und Leistung der Arbeitnehmer/-innen zu ziehen.

Übertragen auf die RFID-Technik bedeutet dies, dass die Einführung von Tags im Betriebsausweis oder in der Kleidung von Arbeitnehmerinnen und Arbeitnehmern mitbestimmungspflichtig ist, da damit theoretisch eine Überwachung möglich ist.

> **Will der Arbeitgeber eine mitbestimmungspflichtige Maßnahme durchführen, so bedarf es hierzu der Einigung mit dem Betriebsrat. Bei Personaldaten, Gesundheitsbelangen, Betriebsänderungen und bei der Planung technischer Anlagen hat der Betriebsrat ein Wörtchen mitzureden.**

Das Gleiche gilt für auf Produkten angebrachte RFID-Tags, die personenbezogene Daten enthalten. Fehlen solche personenbezogenen Daten, werden mit der Technik also lediglich Warenströme besser gesteuert oder verfolgt, so ist im Einzelfall zu klären, ob trotzdem ein Mitbestimmungsrecht vorliegt. Obwohl hier ein unmittelbarer Personenbezug fehlt, ist zu prüfen, ob dieser durch Verknüpfung mit anderen Datenquellen hergestellt werden kann. Hierzu bedarf es einer Prüfung des IT-Systems.

Insbesondere vorgefertigte Module, die geeignet sind Daten miteinander zu verknüpfen, bereiten den Boden für Personalkontrollen. Beispiele hierfür gibt es bereits viele.

Exemplarisch hier einige Module für RFID-Technologie der Firma SAP:

- SAP Auto-ID Infrastructure: Verwaltet und verbindet RFID-Daten und kommuniziert mit anderen Geräten zur automatischen Datenerfassung.

- SAP Event Management: Für RFID-Tags und Electronic Product Codes (EPC); sorgt durch Auto-ID-Daten für Transparenz des Warenbestands, ermöglicht den Austausch zwischen Geschäftspartnern und löst automatisch Alarm aus.

- SAP NetWeaver Portal: Bündelt RFID-Informationen und ermöglicht internen Nutzern sowie Handelspartnern, darauf zuzugreifen.

- ERP-Adapter: Planen Personen- und Materialressourcen und lassen sich in bereits bestehende Logistikabwicklungsprozesse von SAP R/3 (ab Release 4.6C) integrieren.

- SAP NetWeaver Application Server: Verknüpft Daten in der Infrastruktur.

- SAP NetWeaver Exchange Infrastructure: Verknüpft Daten mit SAP- und Nicht-SAP-Komponenten bis über die Unternehmensgrenzen hinaus.

- SAP NetWeaver Mobile: Stellt die technische Grundlage für mobile Lösungen bereit.

Ein Recht des Betriebsrats auf Mitbestimmung hängt also davon ab, ob es möglich ist, mit Einführung der geplanten technischen Maßnahmen Personenbezüge herzustellen. Manchmal ist dies nicht auf Anhieb offensichtlich, manchmal aber auch auf banalem Wege möglich: Ersieht man aus Listen oder anderen Dokumenten, wer wann mit der fraglichen Ware zu tun hatte, kann das Arbeitsverhalten sehr genau rekonstruiert werden. Wird beispielsweise festgehalten, wann und auf welchem Fahrzeug eine Ware ein bestimmtes Lager verlässt, so ist gleichzeitig eine Aussage über denjenigen möglich, der für das Lager verantwortlich war oder der am Steuer des Lkw saß. Dieses Hintergrundwissen stellt den Personenbezug her.

Fazit: Ist es möglich, bei RFID-Anwendungen Rückschlüsse auf Personen zu ziehen, so hat der Betriebsrat das Recht, über die Einführung der technischen Maßnahme mitzubestimmen

6.7. Gesundheitsbelange

Der Betriebsrat hat darüber hinaus auch ein Mitbestimmungsrecht bei Regelungen über den Gesundheitsschutz im Rahmen der gesetzlichen Vorschriften. Dieses Recht erstreckt sich auf alle Maßnahmen, die im Rahmen der Vorschriften des Arbeits- und Gesundheitsschutzes im Betrieb zu treffen sind. In der Praxis kann der Betriebsrat grundsätzlich annehmen, dass er bei drohenden Gesundheitsgefahren und der Frage nach den geeigneten Schutzmaßnahmen ein Recht auf Mitbestimmung hat.

Gesundheitsgefahren durch die Einführung der RFID- Technologie (zB Strahlenbelastung) oder die Änderungen der Arbeitsabläufe und -verfahren (physische und psychische Belastungen) sind bisher nicht dokumentiert. Eine der grundlegenden Aufgaben des betrieblichen Arbeits- und Gesundheitsschutzes ist es dennoch, die sich verändernden Arbeitsbedingungen zu beurteilen und daraus resultierende mögliche Gefahren für die Gesundheit und Sicherheit der Beschäftigten festzustellen.

Die Gesundheit von Menschen kann gefährdet sein durch:

- die Arbeitsstätte, zB neue Verkehrswege durch Tunnelscanner

- den Arbeitsplatz, zB montierbare Lesegeräte oder mobile Terminals

- physikalische und chemische Einwirkungen, zB durch Strahlenbelastung

- Maschinen und Geräte, zB Bildschirm und Lesegeräte

- Arbeitsstoffe, zB Lösungsmittel

- Arbeitsabläufe, Arbeitsverfahren

- Arbeitszeit, zB Nachtarbeit

- unzureichende Qualifikation, zB im Umgang mit neuen Geräten.

Das bedeutet, immer wenn

- ein Bildschirmarbeitsplatz eingerichtet wird (bereits im Planungsstadium),

- Arbeitsplätze und Aufgaben sich grundlegend ändern,

- Beschäftigte wechseln,

- oder Beschwerden auftreten, die sich auf die Bildschirmarbeit zurückführen lassen, dann ist eine erneute Beurteilung der Arbeitsbedingungen fällig.

Die Pflichten des Arbeitgebers sind an verschiedenen Stellen gesetzlich geregelt:

- Der Arbeitgeber muss die Arbeitsbedingungen hinsichtlich einer möglichen Gefährdung der Beschäftigten beurteilen

- Der Arbeitgeber muss an Bildschirmarbeitsplätzen die gesundheitlichen Gefahren beurteilen, insbesondere für das Sehvermögen. Mögliche körperliche Probleme und psychische Belastungen sind ebenfalls zu berücksichtigen

- Der Arbeitgeber muss die getroffenen Maßnahmen des Arbeits- und Gesundheitsschutzes auf ihre Wirksamkeit hin überprüfen und erforderlichenfalls an veränderte Gegebenheiten anpassen

6.8. Planung Technischer Anlagen

Der Arbeitgeber hat den Betriebsrat über die Planung technischer Anlagen rechtzeitig zu unterrichten und sich mit ihm zu beraten, so dass Vorschläge und Bedenken berücksichtigt werden können. Dies soll gewährleisten, dass der Betriebsrat Einfluss nehmen kann, damit Grundrechte, insbesondere der Schutz der Menschenwürde, die freie Entfaltung der Persönlichkeit sowie das Recht auf körperliche Unversehrtheit gewahrt bleiben.

Der Arbeitgeber muss die Einsatzgebiete sowie die technischen Möglichkeiten der RFID-Systeme beschreiben, und er muss die damit verbundenen Ziele aufzeigen. Außerdem ist es erforderlich, die organisatorischen Auswirkungen offen zu legen, einschließlich Hardware, Standorte, Vernetzung und Schnittstellen. Die Gestaltung des Mediums ist dabei unbedeutend. Statt einer Chipkarte kann daher der Datenträger zum Beispiel auch ein Armband sein.

Entscheidend ist, dass die/der Betroffene die Verarbeitung der Daten nicht selbst steuern kann. Zur Gewährleistung der Transparenz ist die/der Betroffene über die Identität und Anschrift der verantwortlichen Stelle sowie in allgemein verständlicher Form über die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden personenbezogenen Daten zu unterrichten. Zusätzlich ist sie/er über die Ausübung ihrer/seiner Rechte zu unterrichten und über die Maßnahmen, die bei Verlust oder Zerstörung des Mediums zu treffen sind.

6.9. Begleitende Kontrolle

Die begleitende Überprüfung und Kontrolle der in den Betrieb integrierten Standard-IT-Systeme mit ihren vielfältigen Schnittstellen ist nur dann für den Betriebsrat erfolgreich, wenn sie umfassend erfolgt, weshalb sie in einer Betriebsvereinbarung ebenso umfassend geregelt sein muss. So ist zu beachten, dass nicht nur die Teilmodule zu betrachten sind, sondern auch alle von ihnen ausgehenden Schnittstellen und ihre Dateninhalte sowie das zugrunde liegende Betriebssystem, das System zum Betreiben des betriebs- und unternehmensweiten Netzes, die Datenbank(en) und die Einbindung in die überbetriebliche Vernetzung. Auch alle Aspekte der Fernwartung und -pflege (evtl. durch externe Dienstleister) sind einzubeziehen.

6.10. Transparentes Verfahren

Um mit Hilfe der Betriebsvereinbarung ein transparentes Verfahren zu gewährleisten, ist die Dokumentation aller Komponenten des RFID-Systems wichtig. Folgende Inhalte komplettieren daher die zusammengestellten Informationen und gehören in den Anhang (die Anlagen) der Betriebsvereinbarung:

- Fachkonzept/Dokumentation des Systems
- Schnittstellenbeschreibung
- Berechtigungskonzept
- Auswertungen
- Hardware
- Standorte

6.11. Datenschutzkonzept

So kann der Betriebsrat auch ein Datenschutzkonzept entwickeln, das mindestens folgende Aspekte behandelt und regelt:

- Welche Daten werden erhoben?
- Definition des verfolgten Zwecks
- Formen der Datenverarbeitung
- Löschfristen
- Beschreibung der Art der Auswertung
- Zugriffsrechte

6.12. Betriebsvereinbarung

Die Liste der in einer Betriebsvereinbarung zu regelnden und zu prüfenden Bereiche ist lang.

Leistungs- und Verhaltenskontrolle
Der gestattete Umfang sowie die Grenzen der betrieblichen Leistungs- und Verhaltenskontrolle sind zu regeln.

Teilaspekte sind:

- Schutz vor lückenloser Überwachung
- Ausschluss des heimlichen Einsatzes von RFID
- Ausschluss der individuellen Auswertung (RFID ermöglicht es, detaillierte Arbeits- und Zeitprofile zu erheben. Ziel sollte sein, dass neben dem Datum und dem Standort des Lesegeräts keine Zeitangaben gespeichert, sondern höchstens grob erfasst werden, um Bewegungs- und Zeitprofile der Beschäftigten zu verhindern)
- Missbrauchsfälle definieren
- Verfahren bei Missbrauch festlegen
- Pseudonymisierung (Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren)

6.13. Ergonomie

Der Aspekt der Ergonomie umfasst die Frage, welche Voraussetzungen notwendig sind, damit die Arbeit als menschengerecht gilt. Arbeit darf nicht schädigen. Arbeit soll erträglich sein; das gesundheitliche Befinden darf nur in zumutbarem Rahmen beeinträchtigt sein.

Damit diese grundsätzlichen Anforderungen sicher gestellt sind, gibt es ergonomische Grundanforderungen für IT-Systeme:

- IT-Systeme müssen die/den Anwender/-in unterstützen, die Arbeitsaufgabe effektiv und effizient zu erledigen (Aufgabenangemessenheit).
- Die Systeme müssen direkt durch Rückmeldung oder auf Anfrage verständlich sein (Selbstbeschreibungsfähigkeit).

- Die Anwender/-innen müssen das System zielgerichtet starten und bedienen können (Steuerbarkeit).
- Das System muss mit den Kenntnissen (Ausbildung, Erfahrung, Konventionen etc.) der Anwender/-innen konform gehen (Erwartungskonformität).
- Das Arbeitsergebnis muss trotz fehlerhafter Eingaben ohne oder mit minimalem Korrekturaufwand erzielbar sein (Fehlerrobustheit).

6.14. Qualifikation und Einschulung

Vor der Einführung eines neuen Systems (hier: RFID-Technologie zusammen mit dem entsprechenden IT-System) benötigen die Nutzer/-innen entsprechende Qualifikationsmaßnahmen und arbeitsplatzbezogene Einweisungen; während der Einführungsphase benötigen sie Hilfestellung. Aber auch im Routinebetrieb stellen sich Situationen ein, in denen fachkundige Hilfe notwendig ist.

Für die Beschäftigten sind Schulungen zur Erlangung der notwendigen Qualifikation wichtige Voraussetzungen, um technisch-organisatorische Neuerungen bewältigen zu können. Nur durch zusätzliche Qualifikation sind die Beschäftigten in der Lage, die neuen Handlungsräume aufgrund der nun veränderten Arbeitsorganisation auszuschöpfen und neue Aufgaben zu erledigen, ohne dies als Belastung zu empfinden.

Inhalte einer Betriebsvereinbarung

- Geltungs- und Anwendungsbereich
- Probephase/Pilotprojekt
- Transparentes Verfahren
- Datenschutzkonzept
- Regelungen zu Leistungs- und Verhaltenskontrolle
- Ergonomie
- Qualifikation und Einweisung der Beschäftigten
- Information der Beschäftigten (Auskunftsansprüche)
- Beratung durch externe Sachverständige
- Kontrollrechte für den Betriebsrat
- Verfahren bei Änderungen (Informations- oder Mitbestimmungsrechte)
- Wirkungsanalyse
- Anlagen/Anhang:
  - Fachkonzept/Dokumentation des Systems
  - Schnittstellenbeschreibung
  - Berechtigungskonzept
  - Auswertungen
  - Hardware
  - Standorte

Sie sollten dazu während der Arbeitszeit die erforderliche Aus- und Fortbildung erhalten. Die Bildungsmaßnahme muss frühzeitig stattfinden. Der Inhalt der Maßnahme und der Kreis der Teilnehmer/-innen sollte mit dem Betriebsrat abgestimmt werden.

Die Qualifizierungsmaßnahmen sind an praktische Aufgabenstellungen und an die Erfahrung der Beschäftigten auszurichten. Die Schulungen müssen methodisch und didaktisch auf die Zielgruppen zugeschnitten sein. Um einen reibungslosen Betriebsablauf zu gewährleisten und die Beschäftigten nicht unnötig zu strapazieren, ist während der Einführungsphase eine interne IT- Hotline bzw. Einführungsunterstützung (Nutzerservice) erforderlich.

Die Aufgaben umfassen:

- Beratung der Beschäftigten
- Betreuung des IT-Systems (Hard- und Software, Wartung, Fehlerbeseitigung usw.)
- Weiterentwicklung des IT-Systems unter Berücksichtigung der Wünsche und Anforderungen der Nutzer/-innen
- Organisation und Durchführung von Schulungen für die Nutzer/-innen
- Organisation und Durchführung von regelmäßigen Konferenzen mit den Nutzerinnen und Nutzern
- ggf. Betreiben einer Hotline.

Zusätzlich zur Qualifizierung und Betreuung der Nutzer/-innen sind weitere Hilfsmittel notwendig. Dazu gehören praxisorientierte Arbeitshilfen, die den Leistungsumfang der Soft- und Hardware genau beschreiben, die Bedienung erklären und auch zum Selbststudium geeignet sind. Zusätzlich sollte eine kurz gefasste Bedienungsanleitung jederzeit verfügbar sein (z.B. durch Aushang). Wichtig sind auch Online-Hilfen für plötzlich auftretende situationsbedingte Fragen und Probleme (Kontextorientierung). Zur leichteren Einarbeitung und Handhabung sind Lernprogramme empfehlenswert.

6.15. Checkliste für den Betriebsrat

Name des Systems?

Name des Herstellers?

Funktionsumfang/Programmfunktionen?

Zwecke (Verfolgung, Inventarisierung, Kommissionierung usw.)?

Betroffene Abteilungen/Mitarbeiter?

Aufstellorte der Scanner?

Welche Objekte werden mit RFID-Tags versehen (Paletten, Waren, Hausausweise usw.)?

Werden Daten der Mitarbeiter wie Namen und Personalnummern im System hinterlegt?

Werden personenbezogene Daten im System so hinterlegt, dass sie eine natürliche Person

identifizieren können, ohne bloß Name oder Personalnummer zu sein?

Welche Daten sind im RFID-Tag gespeichert?

Welche Daten werden gescannt und mit welchen Systeminformationen (Tag, Uhrzeit usw.) ergänzt?

Ist der Hausausweis (falls mit Transponder ausgestattet) vom Scanner lesbar?

Werden Arbeitsplatzdaten im System hinterlegt?

Welche Auswertungen existieren?

An welche Systeme werden Daten übertragen?

Welche Daten werden an welche Systeme übertragen?

Grafische Übersicht des RFID-Systems mit seinen Verbindungen zu anderen Systemen?

Wer hat welchen Zugriff auf welche Daten?

Terminplan für die Einführung?

7. RASTERFAHNDUNG AN DER KASSE
Loss Prevention

Am Ende des Tages muss die Kasse stimmen und nach Ablauf eines Geschäftsjahres bringt die Inventur ans Licht wie viel Ware fehlt. Die Unternehmen suchen nach praktischen Lösungen um unerwünschte Differenzen zu verhindern. „Loss Prevention" verspricht Abhilfe. Dahinter steckt die Idee, Kassen- und Inventurdifferenzen durch eine lückenlose Leistungs- und Verhaltenskontrolle zu verhindern bzw. zu minimieren. Die dafür eingesetzte Software soll im Einzelhandel Betrug und Unterschlagungen an den Kassenarbeitsplätzen aufdecken und unterbinden.

Dies ist dadurch möglich, dass mittlerweile leistungsstarke und kostengünstige Server verfügbar sind. Die Schwierigkeit bei der Suche nach Betrug und Unregelmäßigkeiten der Beschäftigten lag nämlich bisher darin, dass die zu analysierende Datenmenge zu groß war. Heute ist dies weder technisch noch finanziell ein Problem.

7.1. Data Mining – Wie ihre Daten unterminiert werden

Um Inventur- und Kassendifferenzen aufzuspüren, lassen sich mit „Data Mining" riesige Datenmengen innerhalb kürzester Zeit auswerten. Das Programm durchsucht und analysiert die gesamten vorhandenen Daten nach definierten kritischen Ereignissen und Auffälligkeiten. Jede Abweichung vom zuvor festgelegten Normalverhalten wird aufgespürt und festgehalten.

Die Analysemöglichkeiten sind variabel. Sie können sich auf das gesamte Unternehmen, einzelne Filialen oder bestimmte Gruppen konzentrieren; ebenso auf einzelne Beschäftigte oder einen Teil der Beschäftigten; aber auch auf eine Auswahl von Kassengeschäften, zum Beispiel alle Kassen aus den Kinderabteilungen. Möglich sind darüber hinaus alle Auswertungen, die einen besonderen Bezugspunkt haben, zum Beispiel Transaktionen, die einen bestimmten Betrag übersteigen, sich auf definierte Verkaufsartikel beziehen oder zu ausgewählten Tageszeiten getätigt wurden.

7.2. Das Fahndungsnetz der Supermarktketten

Die folgenden Beispiele, die die Rasterfahndung an der Kasse verdeutlichen, sind keineswegs abschließend, sondern können und werden vor allem in der Praxis weiter ergänzt.

Verdächtig sind zum Beispiel mehrfache Anmeldungen an unterschiedlichen Kassen oder auch über dem Durchschnitt liegende An- oder Abmeldevorgänge. Bei der Kassenabrechnung werden die Berechnung der Plus- bzw. Minusdifferenzen nach Markt, Kasse und/oder Bediener für einen vorgegebenen Tag vergleichend herangezogen. Wer abweicht und damit auffällt, ist erst einmal in das Fahndungsnetz der Supermarktkette geraten.

Auch im Umgang mit dem Personalrabatt ist Vorsicht geboten: Beschäftigte, die Personalrabatt unter der eigenen Nummer gewähren oder über dem Durchschnitt liegende Personalrabattaktivitäten aufweisen, kommen zunehmend ins Visier der Software-Fahndung, genauso wie die Kolleginnen und Kollegen, die Einkäufe über oder unter einem bestimmten Betrag vornehmen. Um Vergleichsmöglichkeiten zu schaffen, werden sogenannte Ranglisten der getätigten Einkäufe durch Beschäftigte erstellt. Auch lässt sich der durchschnittliche Personalkauf pro Filiale laufend anhand der jeweils aktuell anfallenden Zahlen ermitteln.

Auch ein Warenumtausch weckt erst einmal den Verdacht des entsprechend eingerichteten Kontrollsystems: Wie häufig ist die durchschnittliche Warenumtauschaktivität im Unternehmen, in der Filiale, in der Abteilung? Auch bezüglich der Gutscheinausgabe und der Einlöseaktivitäten lassen sich Ranglisten erstellen, die sofort offenbaren, wenn eine Filiale oder ein(e) Verkäufer/-in von der Norm abweicht. Stornobuchungen sind ebenfalls geeignet verdächtig zu erscheinen. Stornos lassen sich nach allen in Betracht kommenden Kombinationsmöglichkeiten auswerten.

Der Verdacht der Manipulation, des Betrugs, der Unterschlagung keimt automatisch auf, ohne dass die Betroffenen davon etwas ahnen. So werden beispielsweise Stornos gruppiert nach Zahlungsmitteln (Bargeld, Kredit-/Kundenkarte, Scheck …), nach Beträgen oder nach Bon-, Zeilen-, Summenstornos akribisch ausgewertet und bewertet.

7.3. Kontrolle des Arbeitsverhaltens

Allein auf Basis der täglich anfallenden Daten im Bereich des Kassierens, lässt sich bereits nach einem kurzen Beobachtungszeitraum Wesentliches über das typische Arbeitsverhalten der Beschäftigten ermitteln. Ein solches Programm bewirkt die vollständige und lückenlose Leistungs- und Verhaltenskontrolle der Beschäftigten an den Kassen. Damit ist eingetreten, wovor Datenschützer warnen: Die Leistungs- und Verhaltenskontrolle ist nicht mehr eine aus Unternehmenssicht angenehme Nebenwirkung, sondern das zentrale Einsatzziel der Firmenleitung. Damit ist erstmals die vollständige und kontinuierliche Analyse von personenbezogenen Daten am Arbeitsplatz zum eigentlichen Systemzweck geworden – die Datenverarbeitung in der Arbeitswelt hat eine neue Dimension erreicht.

Das System wird nicht mehr nur eingesetzt, um einzelne schwarze Schafe zu ermitteln, sondern „Loss Prevention" begründet eine Misstrauenskultur, in der alle Kassierer/-innen als potenziell verdächtig gelten, bei erstbester Gelegenheit unbefugt in die Kasse zu greifen. Als Beweis für die Anschuldigung genügt ein irgendwie von der definierten Norm abweichendes Verhalten. Vordergründig muss nicht der Arbeitgeber beweisen, dass er bestohlen oder betrogen wurde, sondern das Kassenpersonal hat die kontinuierliche Beweislast zu belegen, dass es nichts Unrechtmäßiges getan hat.

7.4. Im Dauerkontakt mit dem Arbeitgeber

Nicht nur für die Beschäftigten im Handel, sondern auch für die Kommissionierung halten die technologischen Anwendungen Neues bereit: „Pick-by-Voice" ist ein sprachgesteuertes und auf Spracherkennung basierendes Kommissionierungssystem, durch dessen Einsatz eine durchschnittliche Produktivitätssteigerung von neun bis 15 Prozent erwartet wird. Die Fehlerrate soll gegen Null gehen. Das sind jedenfalls die Erfahrungen, die Experten in Projekten beispielsweise bei „Edeka", „Woolworth Netto" und „Globus" gesammelt haben.

Bei „Globus" ist die Fehlerrate von 0,5 auf 0,04 Prozent gesunken. „Metro Group Logistics" (MGL) erwartet einen Rückgang der Fehlerquote von 0,3 auf 0,05 Prozent. Da Fehler beim Greifvorgang oder beim Abstellen der Ware zu Folgekosten führen, soll das System dafür sorgen, dass dieser Arbeitsabschnitt fehlerfrei läuft. Die Unternehmen versprechen sich von diesem System nicht allein eine Verbesserung der Fehlerrate, sondern auch in Teilbereichen eine Steigerung der Kommissionierungsleistung. Bei der Arbeit mit Hilfe von „Pick-by-Voice" sind die Beschäftigten mit einem Headset (Kopfhörer mit Sprechvorrichtung) und einem kleinem Funkterminal ausgestattet. Ihr Standort lässt sich grundsätzlich über GPS lokalisieren. Die Beschäftigten erhalten ihre Arbeitsaufträge per Kopfhörer und bestätigen die Entnahme von Ware Stück für Stück am Ende eines jeden Arbeitsschrittes an das Kommissionisierungssystem zurück.

7.5. An der elektronischen Leine

Kritisch stellt die britische Gewerkschaft „GMB" die Anwendung dieser „Talkman-Terminals" dar: Die Gewerkschaft macht darauf aufmerksam, dass im Handel immer mehr Beschäftigte mit tragbaren Computern aller Art an die elektronische Leine gehängt werden.

Die Gewerkschaft warnt davor, dass mit der Technik die Beschäftigten nicht mehr nur permanent überwacht werden, sondern auch die Arbeitsbelastung enorm ansteigt. Zugleich schrumpfe der Raum für eigenverantwortliche Tätigkeiten gen Null und der Weg zu einer weiteren Automatisierung sei frei gemacht. Demnach scheine sich ein neues und zusätzliches Überwachungsszenario für die Beschäftigten im Handel anzubahnen.

GMB bedeutet historisch bedingt:

»General Municipal Boilermaker«, übersetzt: allgemeine kommunale Dampfmacher, und nennt sich jetzt: »GMB – Britains General Union«, übersetzt: Britanniens allgemeine Gewerkschaft.

Die kleinen Computer werden, nach einer Beschreibung von „GMB“, wie elektronische Hand- und Fußfesseln für Straftäter auf Bewährung, an Armen getragen (Handgelenk-Terminals). Zusätzlich gibt es einen kleinen Scanner, der an einem Ring an einem Zeigefinger befestigt wird. Eine andere Variante sind Westen, in denen Computer mit Funkverbindung und GPS-Empfängern eingearbeitet sind. Mit dem »Talkman« können die Angestellten über Spracherkennung mit dem Managementsystem kommunizieren (indirekt sprechen). Es können ebenfalls über Spracherkennung Anweisungen und Qualitätskontrollen in Echtzeit eingegeben werden. Integriert sind ein Touchpad-Display (Befehle über Berührung) und ein Head Mounted Display (für ein Auge oder für beide, ausgestattet mit Ohrhörern und einem Mikrofon). Angeschlossen werden kann auch eine Kamera zur Herstellung und Übertragung von Bildern.

7.6. Arbeiten im Galopp

Die genannten elektronischen Geräte dienen in erster Linie dazu, die Tätigkeit der Beschäftigten (hier: die Kommissionierung) zu steuern. Gleichzeitig ermöglicht diese Technik das Verhalten und die Arbeitsleistung der Beschäftigten minutiös zu kontrollieren. So lassen sich aus dem Verkaufsbereich heraus Befehle an die Beschäftigten im Lager darüber erteilen, welche Produkte sie an welchen Stellen entnehmen und in die Regale stellen müssen. Mittels der Minicomputer lässt sich ausrechnen, wie lange die Beschäftigten für ihre festgelegten Wege benötigen, welche Pausen ihnen zustehen, wie lange sie Pausen machen oder sich an bestimmten Orten aufhalten. Die Menschen dürfen dann nur noch das selbstständig entscheiden, was noch nicht berechnet und automatisiert werden kann.

Die Nachfrage bei einem Betriebsrat, in dessen Unternehmen „Pick-by-voice“ getestet wurde, bestätigt die bisherigen Einschätzungen: Einerseits sichere das System eine beständige Routine im Arbeitsablauf. Andererseits sei jedoch derzeit noch unklar, ob das System lediglich eine Art Routenoptimierung beinhalte oder ob die permanenten Geräusche aus dem Headset (das zudem dauerhaft unangenehm am Kopf drücke) die Kolleginnen und Kollegen in der Kommissionierung voran treibe. In jedem Fall stelle das System „Pick-by-voice“ eine gesundheitliche Belastung der Beschäftigten dar, da keine eigenverantwortlichen Entscheidungen mehr möglich seien und sie die andauernden Befehle als belastend und anstrengend empfänden. Entsprechende Forderungen zum Schutz der Mitarbeiter/-innen seien daher auszuarbeiten. Die Forderung, diese Belastungen abzustellen, habe oberste Priorität. Soweit dies nicht vollständig möglich sei, sollten zusätzliche Pausen, entsprechend der Arbeit an Bildschirmgeräten, gefordert werden, um die Mehrbelastung zu kompensieren.

7.7. Geofence-Technik

„Metro“ hat mit der satellitengestützten Überwachung und Steuerung seiner Lkw-Flotte begonnen. Ziele sind dabei unter anderem eine permanente Temperaturkontrolle, die automatische Anvisierung der Fahrzeuge, bevor sie in den Märkten ankommen und der Diebstahlschutz. Ein weiterer Effekt besteht darin, dass sich die komplette manuelle Verplombung der Fahrzeuge erübrigt – und dass natürlich die jederzeitige Ortung der Fahrzeuge und damit der Fahrer/-innen möglich ist. Ergänzt werden diese Funktionen durch die so genannte „Geofence“-Technik. Um die definierten Läden wird eine imaginäre Mauer gezogen. Daher der Name „Geofence“, was in etwa mit Erd- oder Bodenzaun übersetzt werden kann. Passiert das Lieferfahrzeug diesen unsichtbaren Zaun, so erhält der Markt automatisch eine Nachricht.

Dies bedeutet, dass dort vorher bekannt ist, ob beispielsweise ein Fahrzeug in zehn Minuten da sein wird, da der Zaun um den Markt selbst liegt. Wird vor Eintreffen des Lkw, also außerhalb des Zielortes, die Laderampe oder sogar nur die Tür geöffnet, besteht, ähnlich wie bei „Loss Prevention“, automatisch ein Diebstahlverdacht. Der Fahrer muss eine schlüssige Erklärung dafür liefern, weshalb er die Tür außerhalb der autorisierten Bereiche geöffnet hat.

Dies lässt sich dann auch noch anhand der GPS-Daten gegenprüfen. Zusammenfassend ist deutlich, dass im Handel durch die neuen technischen Systeme eine lückenlose Kontrolle der Leistung und des Verhaltens der Beschäftigten möglich ist, sei es im Verkauf, an der Kasse, in der Logistik oder im Lager. Die neuen Technologien bergen ein nicht zu unterschätzendes Rationalisierungspotenzial. Gerade weil diese Veränderungen schrittweise, wahrscheinlich über mehrere Jahre ablaufen, ist vor Beginn der Nutzung von RFID dringend angeraten, eine Betriebsvereinbarung abzuschließen, die Schutzregelungen trifft und die Prozesshaftigkeit der Einführung und Nutzung von RFID berücksichtigt.

7.8. Pick-by-voice

Die Erfahrungen mit „Pick-by-voice" waren unterschiedlich: Einige der Beschäftigten sind offensichtlich schneller geworden und haben sich in den Galopp bringen lassen. Andere, die zuvor bereits vorausschauend gearbeitet haben, wurden durch „Pick-by-voice" eher ausgebremst, da sie nicht »ihren« Rhythmus laufen konnten (das sind die Menschen, die etwas aus dem Regal nehmen und dabei schon halb ins nächste Regal schauen und damit bereits sehr schnell sind), sondern stets warten mussten, bis das System eine neue Order erteilte oder die Bestätigung der Zuordnungsnummer abrief.

Das sind dann auch die Menschen, die eher unglücklich über das System sind, im Gegensatz zu denen, die lieber auf Ansage arbeiten. Die Anstrengungen der Unternehmen zur Effizienzsteigerung kennen keine Grenzen und machen auch vor den Menschen nicht halt. Wer zu viel Pause macht, der fällt auf und ist beim nächsten Jobroulette raus.

Ein RFID-Gesetz wäre notwendig. Darüber hinaus sollten Industrie und Handel sich über Selbstregulierung und Selbstverpflichtung zur umfassenden Gewährleistung des Datenschutzes verpflichten, möglicherweise auch über eine Datenschutz-Zertifizierung. damit die Kunden sicher sein könnten, dass nicht gegen ihren Willen Datenspuren aus ihrem Privatleben verwendet werden. Doch bleibt es bei dieser Freiwilligkeit, so gibt es keine Pflicht, Datenschnüffeleien zu unterlassen und damit letztendlich auch keine Sicherheit für die Kundinnen/Kunden und Arbeitnehmer/-innen. Festzustellen ist, dass zum Thema Datenschutz und RFID noch viel geregelt und geklärt werden muss.

Industrie und Handel ziehen bereits erste Vorteile und wollen Technik ausbauen, aber die Privatsphäre des Menschen als Konsument/-in und Arbeitnehmer/-in, darf hierbei nicht auf der Strecke bleiben. Für die Beschäftigten sind Betriebsvereinbarungen hinsichtlich des Einsatzes von RFID-Technologie die beste Möglichkeit, den Einsatz im Betrieb zu regeln sowie Transparenz hinsichtlich der Verarbeitung ihrer personenbezogenen Daten herzustellen. Für die Konsumentinnen und Konsumenten bleibt, solange gesetzliche Regelungen fehlen, nur die Hoffnung auf eine freiwillige Selbstverpflichtung der Firmen.

7.9. Personenprofile

Viele Daten, wie zum Beispiel Produktinformationen allein für sich, sind datenschutzrechtlich unproblematisch und können für Verbraucher/-innen sowie für das Verkaufspersonal gleichermaßen hilfreich bei der Auswahl der Produkte sein.

Wenn jedoch eine Kundinnen-/Kundenkarte oder ein Mitarbeiter/-innen-Ausweis mit einem RFID-Chip versehen ist, so lassen sich die betreffenden Personen identifizieren, sobald sie am Eingang eines Geschäftes oder an einem anderen Ort ein platziertes Lesegerät passieren. Wenn Verkäufer/-innen sich vom Verkaufsbereich in den Aufenthaltsraum begeben und dabei von Lesestationen erfasst werden, dann lassen sich über die Personen Profile erstellen. In einem Geschäft, Gebäude oder an anderen Plätzen installierte Lesegeräte ermöglichen detaillierte Bewegungsprofile.

Daraus lässt sich erkennen, an welchem Tag zu welcher Uhrzeit und wie lange die Verkäufer/-innen sich in den unterschiedlichen Bereichen aufgehalten haben, wie lange sie für eine bestimmte Wegstrecke gebraucht oder im Aufenthaltsraum Pause gemacht haben.

Diese Daten lassen sich mit denen anderer Systeme, wie der Videoüberwachung oder einem „Loss-Prevention"-System verknüpfen und abgleichen. So könnte beispielsweise eine Auswertung ergeben, dass ein/-e bestimmte/-r Verkäufer/-in jeweils nach einem Einkauf, einem Storno oder einem Nullbon die Kasse verlässt und regelmäßig in einen bestimmten Bereich des Ladens geht. Daraus könnten Schlüsse gezogen werden, die möglicherweise völlig unzutreffend sind.

Im Lagerbereich könnte durch RFID erfasst werden, wie viele Paletten ein/-e Arbeitnehmer/-in in einem bestimmten Zeitraum bewegt hat, wie viele und welche Laster sie/er beladen und welche Wege sie/er dabei zurückgelegt hat. Die Dichte der Daten, die über eine/-n einzelne/-n

Arbeitnehmer/-in erhoben werden kann, ist letztlich abhängig von der Anzahl der Lesestationen. Schnittstellen zu anderen Datenbanken eröffnen Verknüpfungsmöglichkeiten mit weiteren Daten der Arbeitnehmer/-innen. Beispielsweise lässt sich die Anzahl der Ladevorgänge und die Pünktlichkeit bei Arbeitsantritt zueinander in Beziehung setzen.

Die zu stellenden Fragen lauten somit:

- Zu welchem Zweck sollen personenbezogene und beziehbare Daten erhoben, verarbeitet und genutzt werden?
- Welche Daten werden wo über wen erhoben und gespeichert?
- Wer macht was mit welchen Daten?
- Wo werden diese gespeichert, z.B. in einem Data Warehouse?
- Wer hat Zugriff auf die Daten?
- Wie sicher ist das System gegenüber unbefugtem Auslesen?
- Zu welchem Zeitpunkt sollen personenbezogene Daten gelöscht werden?
- An wen werden Daten übermittelt oder weitergegeben?

7.10. Vor Missbrauch nicht gefeit

RFID-Chips sind so klein, dass sie fast überall, zum Beispiel in ein Kleidungsstück eingearbeitet werden können. Die Firma „Benetton" hat bereits RFID-Chips in Kleidungsetiketten eingearbeitet, ohne dass die Käufer darüber aufgeklärt wurden. Datenschützer haben vehement dagegen protestiert, so dass „Benetton" dieses Pilotprojekt eingestellt hat.

»Loss Prevention«

ist eine Software, die von jeder Kassiererin und von jedem Kassierer Profile erstellt. Abweichungen von diesem Profil gelten als ungewöhnliches Verhalten. Das Fischen nach auffälligen Personen soll der Aufdeckung von Verlustquellen, die durch Manipulationen und/ oder Fehlbedienungen von Kassen entstehen, dienen.

Auch in Payback-Karten waren 2003, ohne dass Verbraucher/-innen etwas davon wussten, RFID-Chips integriert. Es gilt daher: Ein verdecktes Anbringen von RFID-Tags und das unerkannte Auslesen von Daten muss unbedingt verhindert werden. Eine andere Variante des Missbrauchs ist die Fälschung der Identität des Lesegerätes. Damit wird einem RFID-Chip vorgegaukelt, dass ein Lesegerät berechtigt ist, die Daten auf dem Chip abzufordern. Beim Übertragen der Daten von dem RFID-Chip auf das Lesegerät besteht dann die Möglichkeit, die Daten abzuhören oder zu verfälschen. Für die Verbraucher/-innen und die Beschäftigten ergeben sich beim Einsatz der RFID-Technologie folglich diverse Risiken (s.u.).

7.11. Konsumentenschutz

An die aufgeführten Risiken, die sich aus dem Einsatz der RFID-Technologie ergeben, schließt die Forderung nach Maßnahmen zum Schutz der Konsumentinnen/Konsumenten und der Beschäftigten unmittelbar an:

- Beschäftigte und Konsumentinnen/Konsumenten müssen wissen, wo RFID-Tags zum Einsatz kommen und was auf diesen gespeichert wird.
- Für Beschäftigte und Konsumentinnen/ Konsumenten muss eindeutig erkennbar und transparent sein, wann durch RFID-Tags Kommunikationsvorgänge ausgelöst werden, die die Verarbeitung personenbezogener Daten zur Folge haben.

Risiken für Verbraucher/-innen

Da die RFID-Systeme berührungslos arbeiten, kann das Auslesen der auf Kundinnen-/Kundenkarten gespeicherten Daten ohne Wissen der betroffenen Person erfolgen.

Bei versteckt an Produkten angebrachten Chips ergreifen Käufer/-innen keine Schutzmaßnahmen, da sie von den an den Produkten angebrachten Chips nichts wissen. Da hilft dann nur ein Gerät, welches RFID-Chips aufspüren kann.

RFID-Tags ermöglichen eine eindeutige Kennzeichnung von einzelnen Gegenständen. Erworbene Produkte können somit weltweit eindeutig einzelnen Personen zugeordnet werden. Voraussetzung ist, dass beim Kauf des gechippten Produktes der Bezug zur Käuferin oder dem Käufer hergestellt und nicht aufgehoben wird.

Durch die Zusammenführung der Informationen aus RFID-Chips mit personenbezogenen Daten, lässt sich das Kaufverhalten einzelner Kundinnen/-Kunden detailliert analysieren. Auf diese Weise lassen sich Kundenprofile erstellen. Präferenzen der Kundinnen/-Kunden für einzelne Produkte, für die Reihenfolge des Besuchs bestimmter Abteilungen sowie für bestimmte Warenpräsentationen können so erfasst und gespeichert werden.

Risiken für Beschäftigte

Da die RFID-Systeme berührungslos arbeiten, kann das Auslesen der z.B. auf Firmenausweisen gespeicherten Daten ohne Wissen der betroffenen Person erfolgen. RFID-Chips könnten versteckt in Berufsbekleidung eingearbeitet werden. Auch hier ergreifen die Beschäftigten, da sie von der Existenz des Chips nichts wissen, keine Schutzmaßnahmen.

Die weltweit eindeutige Kennzeichnung von Produkten ermöglicht es, z.B. festzustellen, wann während der Herstellung oder des Versands das einzelne Produkt Schaden genommen hat. Durch die Verknüpfung dieser Daten mit Schichtplänen ist festzustellen, wer den Schaden verursacht hat, so dass Schadenersatzansprüche an die/den Beschäftigte/-n gestellt werden können.

Durch die Zusammenführung der Informationen aus RFID-Chips mit personenbezogenen Daten lassen sich Bewegungsprofile erstellen. Leistungsund Verhaltenskontrolle ist möglich.

- Personenbezogene Daten auf RFID-Tags von Beschäftigten aber auch von Verbraucherinnen/Verbrauchern dürfen nur so lange gespeichert bleiben, wie dies zur Erreichung des Zwecks erforderlich ist. Nach Zweckerreichung sind sie zu löschen.

- Für die Beschäftigten muss die Möglichkeit zum Lesen der beispielsweise auf Firmenausweiskarten gespeicherten Daten gegeben sein. Das Auskunftsrecht steht selbstverständlich auch den Konsumentinnen und Konsumenten zu.

- Käuferinnen und Käufer müssen Daten auf Produkten mit RFID-Tags nach dem Kauf löschen können. Zudem sollten wirksame Blockierungsmaßnahmen (z.B. eine abschirmende Einkauftasche) angeboten werden, damit sie nicht der Gefahr ausgesetzt sind, bei Verlassen des Ladens mit gechippten Produkten doch noch ausgelesen zu werden.

- Die Vertraulichkeit der von Beschäftigten sowie von Kundinnen und Kunden gespeicherten und der übertragenen personenbezogenen Daten muss durch wirksame Verschlüsselungstechnik sichergestellt sein.

- Grundsätzlich sollten Personenverfolgungen und die Erstellung von Profilen nicht gestattet sein, weder bei den Beschäftigten, noch bei den Verbraucher/-innen. Das Augenmerk muss sich darauf konzentrieren, einen kontrollierbaren Einsatz von RFID-Technologie zu ermöglichen und keine Kontrolle durch RFID zu schaffen!

7.12. Datendiebstahl

Um sich vor den von der RFID-Technologie ausgehenden Gefahren zu schützen, kommen mehrere Möglichkeiten in Betracht: Da käme zunächst das Blockieren, also das Stören des Funkverkehrs in Frage, zum Beispiel durch aktive Störsender, die man in der Tasche mit sich führen kann. Aber auch eine Art Faradayscher Käfig um einen RFID-Chip, der diesen abschirmt, wäre denkbar, zum Beispiel in Form einer Einkaufstasche.

Die „Metro Group" zum Beispiel bietet ihren Kundinnen und Kunden die Möglichkeit, den auf den RFID-Chips gespeicherten individuellen EPC-Code zu löschen. Der Kunde kann dann per Tastendruck den Chip deaktivieren und, so die „Metro Group", dauerhaft unbrauchbar machen. Allerdings muss geklärt sein, was mit den auf den Chips gespeicherten Echtheitszertifikaten und den Garantieansprüchen im Falle einer Zerstörung geschieht.

Das Deaktivieren der Chips bietet keinen sicheren Schutz, wenn sie nur zeitweise deaktiviert und später durch spezielle Lesegeräte wieder aktiviert werden können. Die Industrie bietet so genannte Clipped Tags an. Dies sind RFID-Etiketten, die es den Konsumentinnen und Konsumenten ermöglichen, die Etiketten mechanisch zu verändern, so dass die Antenne des RFID-Chips zerstört wird. Das soll entweder durch das Abziehen einer Folie, das Rubbeln auf dem Etikett oder das Wegknicken einer vorperforierten Bruchstelle erfolgen. Bei allen drei Varianten soll der Chip jedoch voll funktionstüchtig bleiben. Mit einer Zusatzantenne soll er wieder reaktiviert werden können. Das ist zum Beispiel dann erforderlich, wenn Ware zur Reparatur eingeschickt werden muss. Weitere Produkte, die es ermöglichen sollen, sich direkt vor dem unbefugten Auslesen der Chipdaten zu schützen sind unter http://www.foebud.org zu finden.

7.13. Kein Konsum ohne Datenschutz

Wird die RFID-Technologie eingesetzt, so ist Datenschutz unverzichtbar. Die technischen Mittel sind vorhanden, um zum Beispiel die Tag-Daten verlässlich gegen Angriffe zu schützen. Allein der Preis lässt viele Firmen vor Schutzmaßnahmen zurückschrecken. Ein fahrlässiger Umgang mit Daten sowie fehlender oder ungenügender Datenschutz sind nicht akzeptierbar. Jeder technische Fortschritt, der geringere Bestandsreserven und weniger Regallücken durch bessere Planbarkeit ermöglicht, der die Personal- und Lagerkosten verringert und der die Kundenorientierung sowie den Service erhöht, verschafft den Unternehmen einen Wettbewerbsvorteil gegenüber den schlechter ausgerüsteten Konkurrenten.

Eine Bedingung für die erfolgreiche Nutzung von RFID entlang der Liefer- und Wertschöpfungskette, der „Supply Chain", ist eine gemeinsame Ausrichtung der Standardisierungsbemühungen von Industrie, Handel und Logistik. Die Schaffung der technischen und organisatorischen Voraussetzungen für eine aussichtsreiche Umsetzung der RFID-Technologie wird in den dominierenden Unternehmen mit großem Einsatz vorangetrieben. Prognosen der Unternehmensberatung McKinsey besagen, dass im Jahr 2010 jede zweite Palette, jede dritte (Um-)Verpackung, aber nur jeder zwanzigste Artikel mit einem RFID-Tag ausgestattet sein wird. Technikanwendungen wie Videoüberwachung, Pick-by-voice, Loss Prevention sind vielerorts schon alltägliche Praxis, GPS und Geofence werden sich ebenfalls etablieren.

8. TECHNISCHE ANALYSE RFID-BEZOGENER ANGSTSZENARIEN

Die Vorstellung einer Integration von Chips in alle uns umgebenden Objekte sowie die damit mögliche geräuschlose Kommunikation von Objekten untereinander rufen bei vielen Unbehagen hervor. So hat zB die Gesellschaft für Informatik eine Warnung vor der Technologie formuliert und einen Maßnahmenkatalog aufgestellt, „um die potentiellen Gefahren von Transpondern für die Bürger und die Gesellschaft auf ein Minimum zu reduzieren." (Pohl 2004)

Selbst industrienahe Studien belegen negative Reaktionen auf potenzielle Folgen der RFID-Technik. Dabei steht die Angst vor einem Verlust der Privatsphäre im Vordergrund und dominiert andere potenzielle Auswirkungen der Technologie auf Gesundheit und Arbeitsmarkt. (Tabelle 1: Auswahl RFID-bezogener Ängste in der öffentlichen Wahrnehmung)

Wahrgenommene Ängste	**Beschreibung**
Erfassen von Besitz	unbemerktes und ungewolltes Auslesen des persönlichen Besitzes durch Dritte
Tracking von Personen	Möglichkeit, dass Lesegeräte von Menschen unbemerkt auf Objekte zugreifen und auf diese Weise pseudonyme oder identifizierte Bewegungsprofile entstehen sowie Aufenthaltsorte von Personen kurz- und langfristig nachvollzogen werden
Erheben sozialer Netzwerke	automatisiertes Erheben von Beziehungen zwischen Menschen
unkontrollierbarer Technologie-Paternalismus	Möglichkeit, durch die Objekt-Erkennung der Technologie selbst kleinste Fehltritte systematisch und automatisch zu sanktionieren
langfristige objektbezogene Verantwortlichkeit	Angst vor einer eins-zu-eins Zuordnung von Personen zu ihren Objekten, die mit einem potenziellen Verantwortlich-Machen für den Missbrauch oder Verbleib von Objekten einhergeht

Im Folgenden werden einzelne Angriffszenarien diskutiert, die konkrete Ausprägungen der in Tabelle 1 beschriebenen Ängste darstellen.

8.1. Unautorisierte Erfassung von Besitz

Die Angst, dass Fremde unbemerkt Informationen über den eigenen Besitz erwerben könnten, ist der Furcht vor Überwachung zuzuordnen. Die fehlende Kontrolle über den Informationsfluss ist eine Einschränkung der informationellen Selbstbestimmung. Dritten wird potenziell der Besitz von Objekten wie Medikamente oder den Intimbereich betreffende Produkte bekannt.

Technisches Angriffsmodell

Für das Auslesen des auf einem Tag gespeicherten EPCs (Electronic Product Code) kann entweder der Tag direkt ausgelesen oder Kommunikation in der nachgelagerten IT-Infrastruktur abgehört werden. Tag direkt auslesen:

Für den Einsatz im Einzelhandel sind Tags der Klasse 1 vorgesehen. Diese Tags besitzen keine Mechanismen, um den Lesezugriff auf autorisierte Parteien zu beschränken. Die einzige beim Lesen zu überwindende Hürde ist die Entfernung zum Tag. Der Frequenzbereich von 13.56 Megahertz war jahrelang ausreichend, funktioniert jedoch nur im Nahfeld des Lesegerätes (maximal 3,5 Meter). Für den praktischen Einsatz im Handel wird derzeit jedoch eine Kommunikationsfrequenz im Bereich von 865 bis 868 Megahertz vorgeschlagen, mit unter optimalen Bedingungen einer praktisch zu überwindenden Distanz von 6–8 Metern, bei der das unbemerkte Auslesen von Tags möglich wäre.

Nachgelagerte IT-Infrastruktur nutzen: In RFID Anwendungen werden Informationen von RFID Tags durch Reader ausgelesen und an nachgelagerte Anwendungen weitergeleitet, welche zum Teil über das Internet miteinander interagieren. Die dabei verwendeten Kommunikationskanäle weisen mitunter Schwachstellen auf. Beispielsweise werden EPC-Codes unverschlüsselt im Internet übermittelt, wenn der Object Name Service (ONS) zum Auffinden von objektbezogenen Informationen genutzt wird.

Solche und ähnliche Schwachstellen könnten von Angreifern genutzt werden, um von Dritten ausgelesene EPC-Codes zu erfahren. EPC interpretieren: Gelingt es einem Angreifer, die Identifikationsnummer (EPC) eines Tags auszulesen, muss er diese interpretieren können. Die Produktart (Objektklasse) ist im EPC kodiert, sein Aufbau ist öffentlich bekannt. Die Zuordnung des Nummernteils ist nicht in öffentlichen Listen gespeichert, derartige Listen könnten aber erstellt werden, indem die Nummern im Laden erhältlicher Produkte ausgelesen und gespeichert werden. Parteien mit Zugang zu im Aufbau befindlichen EPC Information Services könnten die Produktinformationen auch über diese Systeme erhalten.

Gegenmaßnahmen

Eine permanente Deaktivierung der Tags durch die vorgesehene Kill-Funktion würde die meisten Angriffszenarien unmöglich machen, weil deaktivierte Tags sich nicht auslesen lassen. Ein Nachteil der Kill-Funktion ist, dass wünschenswerte Anwendungen verhindert werden. Hier wäre vielleicht ein Passwortschutz oder ein Hash-Lock Verfahren sinnvoll, welche die volle Kontrolle über Tags in den Nutzerbereich verlagern würden. Möchten Kunden intelligente Dienste oder Heimanwendungen nutzen, oder Garantie- und Recycling-Ansprüche geltend machen, so würden sie an der Leseschnittstelle ein persönliches Passwort eingeben. Bezogen auf das Tracking könnten Kunden in Einkaufspassagen oder Läden am Eingang gefragt werden, ob sie eine Personalisierung der Leistung wünschen. Wenn ja, werden sie aufgefordert, sich zu authentifizieren und können die Leistung in Anspruch nehmen. Lehnen sie dies ab, so bleiben die eigenen Tags still.

8.2. Tracking von Personen

Tracking bezieht sich auf die Angst vor der Überwachung der eigenen Bewegung bzw. der langfristigen und unmittelbaren Nachvollziehbarkeit von Aufenthaltsorten. Allgemein kann man Tracking innerhalb eines Ladens, innerhalb einer städtischen Infrastruktur (z.B. einem Einkaufszentrum), in einer Region, oder überregional unterscheiden. Die räumliche Skalierung bezeichnet man als Granularität, von fein bis grob.

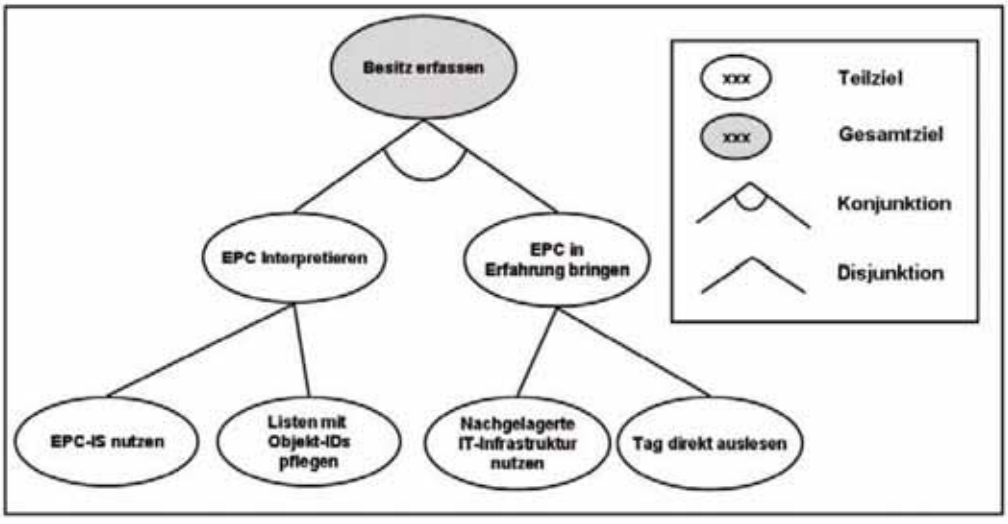

Abbildung 1: Abstrakter Attack-Tree für unautorisiertes Auslesen von RFID-Tags

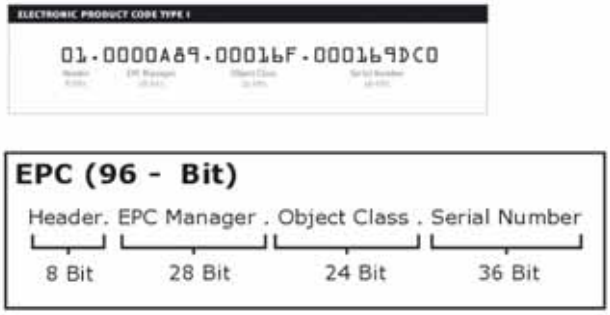

Abbildung 2: Abbildung 2: Aufbau des Electronic Product Code (Variante SGTIN-96)

Technisches Angriffsmodell

Das Angriffsmodell ist in Abbildung 3 dargestellt.

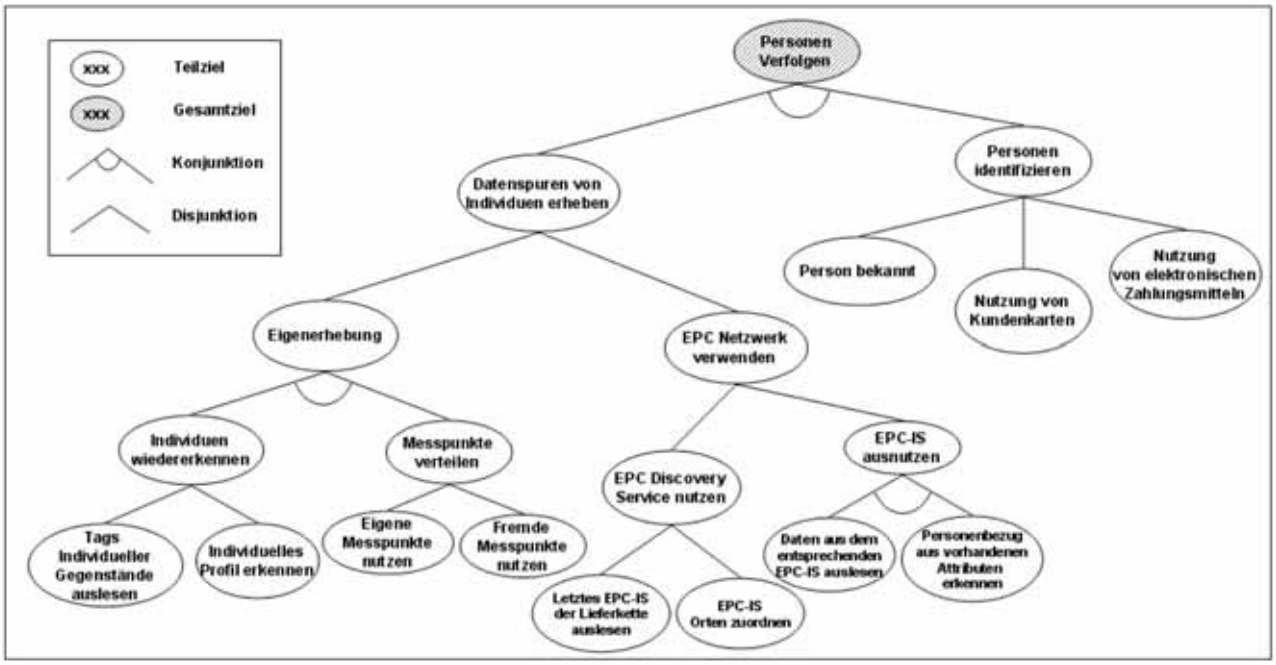

Abbildung 3: Abstrakter Attack-Tree zum Erstellen von Bewegungsprofilen

Gegenmaßnahmen

Wenn Unternehmen über eigene Messpunkte verfügen, kann die Sammlung individueller Daten nur schwer durch technische Maßnahmen verhindert werden. Ebenso ist eine Verknüpfung mit Personendaten nur schwer einzudämmen.

Alternativ zu einer freiwilligen Selbsteinschränkung könnte das Erheben von Bewegungsprofilen gesetzlich eingeschränkt werden. Die Granularität der Readerdaten ließe sich reduzieren. Gäben die Reader (oder die dazu gehörige Middleware) standardmäßig nur zeitlich aggregierte Zeitstempel von Objekteinlesungen weiter, so würde ein Tracking zwar für logistische Zwecke noch ausreichen, ein Personen-Tracking jedoch einschränken. Ebenso möglich ist, dass Kunden ein Privacy-Profil anlegen (beispielsweise im Zusammenhang mit ihrer Kundenkarte), in dem sie bestimmen, welche Daten über sie erhoben werden dürfen.

Vorschläge sind unter dem Begriff „Identitätsmanagement" im E-Commerce Umfeld bereits häufig gemacht worden Tracking-Vorhaben ohne eigene Messpunkte sind auf die Nutzung des EPC Netzwerks angewiesen. Durch restriktive Zugriffsrechte oder die Nichtweitergabe von lokalen Bewegungsprofilen kann die Bedrohung hier eingedämmt werden.

Geht ein Objekt in den Besitz einer Privatperson über, sind auf dieses Objekt bezogene Daten stärker (vor unkontrolliertem Zugriff) zu schützen. Besitzer eines Objektes sollten darüber hinaus Einfluss auf die Festlegung der Zugriffsrechte haben. Für die Zugriffsrechte sind Rollen, Attribute und Dienste zu definieren, für die der Zugriff eingeschränkt werden kann. Dabei ist darauf zu achten, dass Angreifer keine privilegierten Rollen erlangen können. Definiert man beispielsweise eine Rolle für in das Handelsregister eingetragene Firmen, so ist zu bedenken, dass auch Privatpersonen mit geringem Aufwand (durch Gründung eines Gewerbes) diese Rolle einnehmen können.

Zur Eindämmung von Tracking-Ängsten muss der Zugriff auf Informationen darüber, wo sich ein Produkt wann befunden hat, beschränkt werden. Diese Informationen lassen sich aber zum Teil indirekt aus anderen Attributen gewinnen. Beispielsweise lässt sich der Zeitpunkt des Verkaufs auch durch ein Verfallsdatum oder das Herstellungsdatum eingrenzen.

8.3. Erheben sozialer Netzwerke

Hier geht es um das Szenario, dass Unbefugte oder Befugte prüfen können, wer mit wem wann und wo Kontakt hat. Dies kann insbesondere im Rahmen der Strafverfolgung oder Prävention, aber auch im Marketing oder aus persönlichen Motiven heraus von Interesse sein. Es ist nur für solche Instanzen sinnvoll, welche diese Assoziationen nicht leichter auf anderem Wege herstellen können, beispielsweise über soziale Verbindungen und direkte Beobachtungen.

Das Erheben sozialer Netzwerke fußt auf der Annahme, dass Personen, die wiederholt oder über längere Zeit gemeinsam unterwegs sind, eine soziale Verbindung zueinander haben. Dieser Angriff schließt also das Tracking ein.

Gegenmaßnahmen

In der Strafverfolgung oder Prävention sind die Bürger insbesondere vor Fehlern in der Erhebung sozialer Verbindungen zu schützen. Die Herausforderung besteht darin, keine falschen Schlüsse aufgrund von örtlichen Gemeinsamkeiten zu ziehen, sie könnten auch durch ähnliche Arbeitswege entstehen. Die Methode sollte in der Strafverfolgung oder Prävention gesetzlich geregelt werden.

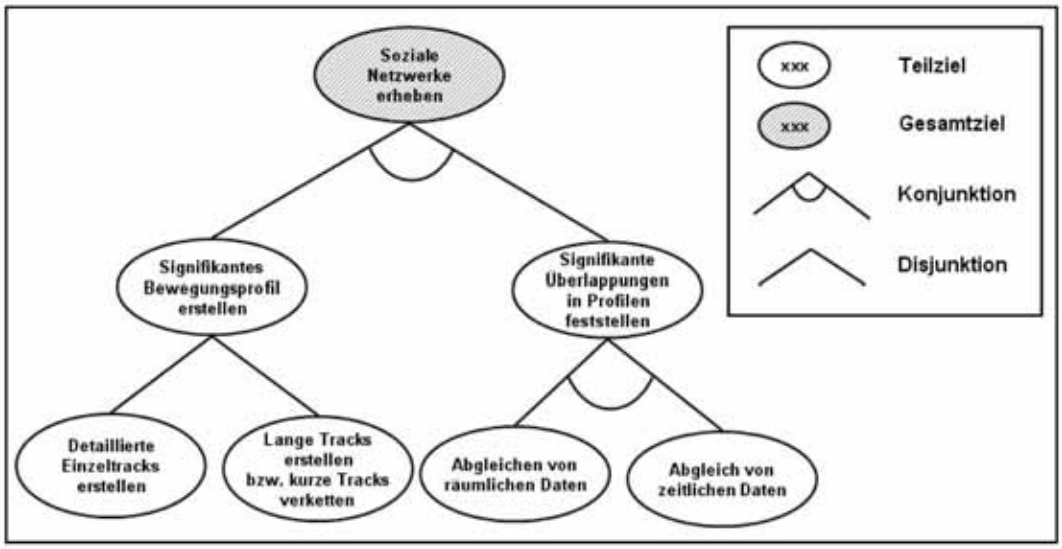

Abbildung 4: Abstrakter Attack-Tree zum Erheben sozialer Netzwerke

Um ein solches Szenario generell abzuwenden, müssten objektbezogene Daten zur Erstellung von Tracks im Hinblick auf Ort, Zeit und Speicherfristen sparsam gespeichert werden. Technologiepaternalismus Geringfügige Fehltritte und ungewöhnliche Verhaltensweisen könnten durch Maschinen automatisiert erkannt, gemeldet oder sogar geahndet werden, wodurch ein Gefühl ständiger Kontrolle und Bevormundung entstehen könnte. Derartige Kontrollen gibt es schon jetzt, zum Beispiel Warnsignale beim unangeschnallten Autofahren.

In Zukunft könnte ein Alarmsignal ertönen, falls Ware in ein falsches Regal zurückgestellt wird. Ähnlich könnte Fehlsortierung bei der Mülltrennung oder bei Veranstaltungen das unerwünschte Mitführen von Lebensmitteln überprüft werden. Einsparungen aus diesen Maßnahmen sind den Kosten gegenüberzustellen.

Technisches Angriffsmodell

Für diesen Angriff ist es notwendig, Fehlverhalten erstens automatisch festzustellen und zweitens zu ahnden.

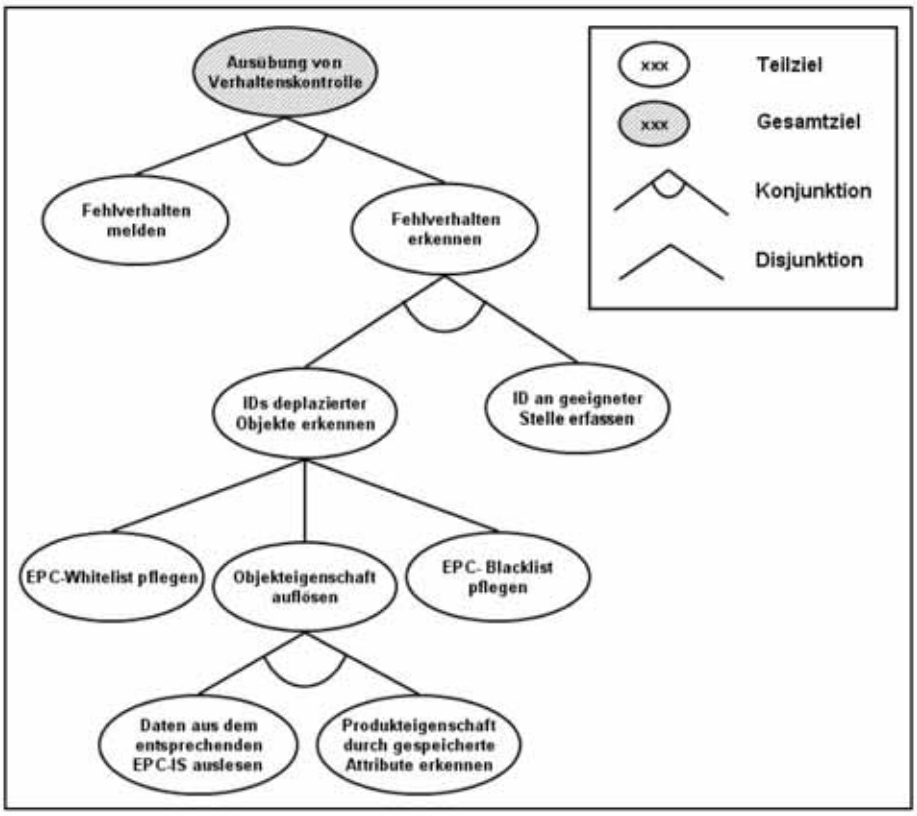

Abbildung 5: Abstrakter Attack-Tree für die Ausübung von Verhaltenskontrolle

Bei gesetzlich nicht strafbarem Fehlverhalten würde die Ahndung ohne rechtliche Mittel erfolgen, beispielsweise durch Bloßstellung (Regale, die bei Fehlsortierung Warnsignale auslösen). Handelt es sich um gesetzlich erfasste Kleinstdelikte, könnten aber auch Strafzahlungen eingefordert werden.

Gegenmaßnahmen

Sind beim Angriff (zur Klassifikation von Objekten) Daten aus dem EPC Netzwerk notwendig, wären auf dieser Ebene technische Abwehrmaßnahmen denkbar. Zugriffsrechte auf objektbezogene Daten könnten stark eingeschränkt werden. Insbesondere wenn das Objekt einer Privatperson gehört, muss überlegt werden, inwieweit ein Zugriff auf diese Objektinformationen überhaupt noch rechtens ist. Zur Gewährleistung der informationellen Selbstbestimmung wäre es ferner wünschenswert, wenn diese Einschränkungen durch den Besitzer konfigurierbar wären. Derartige Beschränkungen sind jedoch ungeeignet, um staatlichen Zugriff zu verhindern.

Viele Anwendungsfälle des Angriffs lassen sich über einfache Blacklists realisieren, Schutzmaßnahmen im EPC Netzwerk würden nicht greifen, weil gewisse Informationen, wie Hersteller und Objektklasse, bereits im EPC codiert sind. Die Zuordnung der Objektklassen zu realen Produkten ist zwar gegenwärtig nicht öffentlich bekannt, aber entsprechende Datenbanken befinden sich im Aufbau. Eine Alternative zur Abwehr dieser Angriffe ist, das Auslesen der RFID-Tags durch eine Abschirmung oder Deaktivierung zu verhindern.

8.4. Personen für Objekte verantwortlich machen

Die Möglichkeit, Objekte bestimmten Personen zuzuordnen, kann in mehreren Fällen von Interesse sein. Für den Staat ergeben sich über den hier diskutierten Angriff erweiterte Möglichkeiten für die Strafverfolgung oder Prävention. Werden an dem Schauplatz eines Verbrechens Gegenstände gefunden, sind damit in Verbindung zu bringende Personen grundsätzlich verdächtig oder könnten wichtige Zeugen sein. Für Betreiber öffentlich zugänglicher Anlagen (Einkaufspassagen, Schwimmbädern oder Parkanlagen) entstehen Reinigungskosten für von Besuchern verursachte Verschmutzung. Um die Verantwortlichen zur Rechenschaft zu ziehen, müssten die in Abbildung 6 visualisierten Teilziele erreicht werden.

Technisches Angriffsmodell

Das technische Angriffsmodell ist in Abbildung 6 dargestellt.

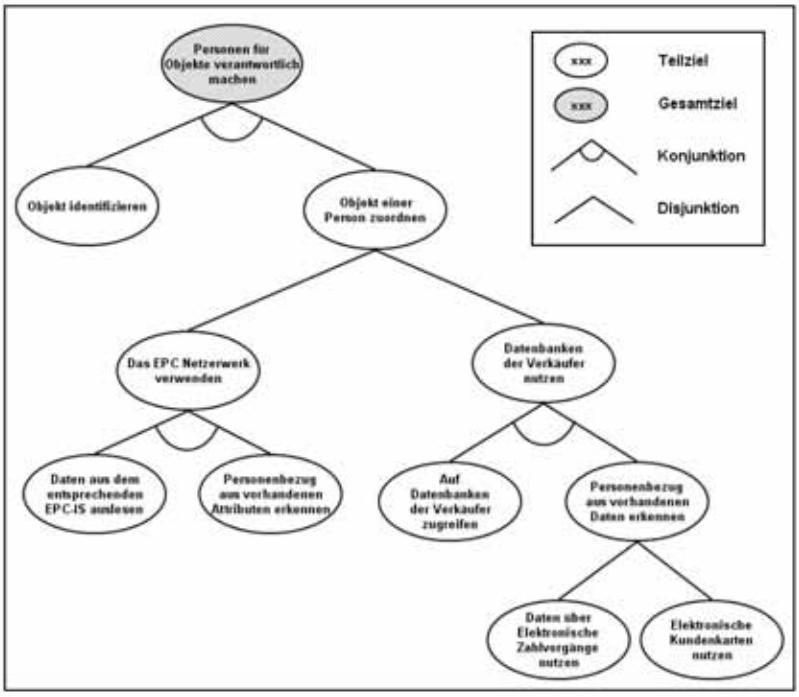

Abbildung 6: Abstrakter Attack-Tree für das Vorhaben, eine Person für ein Objekt verantwortlich zu machen

Gegenmaßnahmen

Um den Angriff abzuwehren, sind zwei Strategien denkbar. Einmal, das Auslesen von Objekt-IDs zu verhindern. Um auch mächtige Angreifer wie den Staat abzuwehren, muss dafür der Speicherinhalt auf dem Tag zerstört werden. Eine Deaktivierung des Chips mittels eines Passworts genügt nicht, da Laboratorien die Informationen dennoch auslesen könnten. Schwächere Angreifer (wie Betreiber öffentlicher Anlagen) könnten jedoch bereits durch eine Deaktivierung ohne Löschung abgewehrt werden.

Alternativ wäre der Angriff abzuwenden, indem die Verknüpfung von vollständigen EPCs mit Personendaten verhindert wird. Tritt der Staat als Angreifer auf, ist sein Zugriff möglicherweise rechtlich gesichert. Einschränkungen der Zugriffsrechte seitens der Datenbankbetreiber sind gegen diesen Angreifer somit wirkungslos. In diesem Fall können die Daten nur durch Verzicht auf die Speicherung geschützt werden. Zwar ist für die Abwicklung von Garantiefällen und Produktrückrufen eine Speicherung von Objekt- Personenbezug gewünscht, allerdings wäre zu diskutieren, wie lange und in welchem Präzisionsgrad eine Speicherung stattfinden kann und soll. Denkbar ist, dass der Seriennummernteil eines EPCs beim Verkauf eines Produktes nicht vollständig gespeichert wird.

Quelle: Sarah Spiekermann,Holger Ziekow, Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V., http://www.fiff.de

9. RFID UND KRYPTOGRAPHIE (VERSCHLÜSSELUNG)

Mit der zunehmenden Verbreitung von RFID-Systemen, die eine kontaktlose automatische Erfassung von Daten erlauben, wächst die Bedeutung von Datenschutz und Datensicherheit. Für sicherheitsrelevante Anwendungen können kryptographische Verfahren den Schutz der übertragenen Daten gewährleisten.

Die automatische Identifikation über Funk, die die Grundlage der RFID-Technik bildet, wurde erstmals 1940 im militärischen Bereich zur Unterscheidung eigener und feindlicher Flugzeuge eingesetzt. Harry Stockman beschrieb in seinem Paper „Communications by Means of Reflected Power" einige Jahre später die Idee, reflektierende Energie in der Kommunikationstechnik zu nutzen. Mit der fortschreitenden Entwicklung der Mikroelektronik eröffnet die RFID-Technik heute ein weites Feld von Anwendungsszenarien.

Während erste Anwendungen im zivilen Bereich bis Ende der 70er Jahre zunächst die Identifikation von Nutztieren ermöglichten, hat RFID in den letzten 35 Jahren fast unbemerkt Einzug ins tägliche Leben jedes Einzelnen gefunden.

9.1. Kryptographische Methoden auf RFID-Systemen

Die Einsatzmöglichkeiten werden einerseits von den technischen Gegebenheiten wie Speicherkapazität und Reichweite, andererseits vom damit verbundenen Kostenfaktor begrenzt. Ein Konsumgut von geringem Warenwert mit einem 20 Cent teueren Chip zu versehen, wäre beispielsweise nicht sinnvoll. In dem Paper RFID Systems, Security and Privacy Implications [SWE03] des MIT wurde eine Kostengrenze für Tags (auch Transponder genannt) von 5 Cent ermittelt, um eine Durchsetzung der RFID-Technik am Massenmarkt erreichen zu können. Voraussetzung für das Erreichen dieser geringen Stückkosten wäre jedoch die Verwendung einfachster Read-Only-Tags, modernster Technologien und Produktionsverfahren und ein sehr großes Produktionsvolumen. Die technische Möglichkeit, ein Produkt weltweit eindeutig zu identifizieren, birgt nicht nur Vorteile, sondern wirft gleichzeitig die Frage nach Datenschutz und Datensicherheit auf. Kryptographische Verfahren bieten eine Möglichkeit zur Absicherung übertragener und gespeicherter Daten vor unbefugtem Zugriff, müssen jedoch unter Berücksichtigung der besonderen Eigenschaften von RFID-Systemen betrachtet werden.

9.2. Bedrohungsanalyse

Im Gegensatz zu anderen Systemen erfolgt bei RFID eine Identifikation ohne Berührung und ohne Sichtkontakt. Daher ist es notwendig zu analysieren, welche möglichen Angriffsarten auftreten können, um diese durch geeignete Schutzmechanismen zu verhindern.

- Abhören der Luftschnittstelle, um durch Wiedervorspielen der Daten einen echten Datenträger vorzutäuschen,
- unautorisiertes Auslesen des Datenträgers, um dessen Inhalt zu verändern oder zu duplizieren,
- Einbringen eines fremden Datenträgers in das Lesefeld, um Echtheit vorzutäuschen.

Das Ergebnis der Bedrohungsanalyse entscheidet über die Wahl eines geeigneten kryptographischen Verfahrens.

9.3. Kryptographische Verfahren

Bei RFID-Systemen ist insbesondere die Authentifizierung von Tags durch das Lesegerät und umgekehrt von Bedeutung. RFID-Systeme müssen beim Erfassen eines Tags dessen Identität überprüfen, um festzustellen, ob dieses Tag zur Teilnahme berechtigt ist. Eine weltweit eindeutige Regelung zur Vergabe der ID-Nummern (Seriennummern), wie es z. B. in Form des Electronic Product Code (EPC) vorgeschlagen wird, bietet einen gewissen Schutz vor gefälschten Tags. Damit kann das Auftauchen nicht vergebener Nummern oder von Duplikaten (Cloning) in manchen Anwendungsfällen erkannt werden. In den übrigen Fällen ist eine Authentifizierung notwendig.

Passwortschutz

Ein einfaches Verfahren zur Authentifizierung des Lesegeräts gegenüber dem Tag ist der Passwortschutz. Das Passwort, das typischerweise eine Länge von 8, 24 oder 32 Bit besitzt, ist nur dem Lesegerät und dem Tag bekannt und wird zum Beginn der Datenübertragung an das Tag gesendet und von diesem überprüft. Stimmt es mit dem im Tag gespeicherten Passwort überein, gewährt dieses den Zugriff auf seine Daten.

Dieser Zugriff kann sich bei aufwändigeren Systemen auf einzelne Speicherbereiche beziehen, so dass mittels einer Schlüsselhierarchie komplexere Sicherheitsmechanismen realisiert werden können. Da das Passwort bei jeder Authentifizierung über die Luftschnittstelle übertragen wird, kann ein Angreifer es abhören und dadurch auf die Daten des Tags zugreifen. Abhilfe schafft die Verwendung variabler Passworte, die sich nach jeder Authentifizierung ändern. Dies setzt ein beschreibbares Tag voraus. In einer Anwendung, in der nur eine beschränkte Anzahl von Zugriffen auf das Tag erforderlich ist, kann hierzu eine Liste von Einmalpasswörtern eingesetzt werden, die dem Tag und dem Lesegerät bekannt sein muss. Beispiele für solche Anwendungen mit beschränkter Zugriffszahl wären Eintrittskarten zu Fußballspielen oder Konzertabonnements.

Ein Authentifizierungsverfahren, das eine größere Sicherheit gegen unautorisiertes Auslesen bietet, ist das Hash-Lock-Verfahren (Abb. 1).

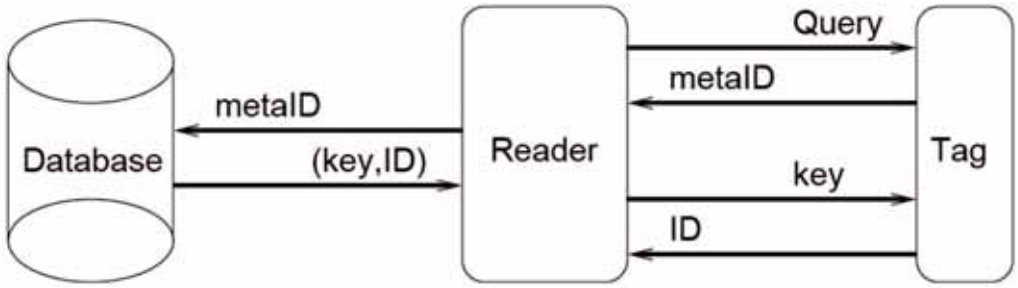

Abbildung 1: Hash-Lock-Verfahren

Hash-Lock-Verfahren

Bei diesem Verfahren werden so genannte Einwegfunktionen eingesetzt, die sich mit geringem Aufwand berechnen, jedoch nur mit sehr hohem Aufwand umkehren lassen. Vor dem erstmaligen Beschreiben des Tags wird ein Paar erzeugt und im Lesegerät gespeichert, das aus einem Schlüssel und dem dazugehörigen so genannten Hash besteht, der mittels der Einwegfunktion berechnet wird.

Dieser Hash, der im Zusammenhang mit dem Hash-Lock-Verfahren auch als metaID bezeichnet wird, wird zusätzlich im Tag gespeichert. Bei der Authentifizierung überträgt zunächst das Tag den Hash an das Lesegerät. Dieses sucht in seiner Datenbank den dazugehörigen Schlüssel und überträgt diesen an das Tag. Das Tag berechnet mittels der Einwegfunktion einen Hashwert aus dem empfangenen Schlüssel und vergleicht ihn mit dem gespeicherten Hash. Stimmen sie überein, wird der Zugriff auf die Daten gewährt. Das Hash- Lock-Verfahren ist für viele Anwendungen als Schutz ausreichend, erfordert jedoch die Fähigkeit des Tags, die Einwegfunktion zu berechnen. Damit ist das Tag aufwändiger und teurer als ein Tag, das nur einen einfachen Passwortschutz bietet. Da außerdem der zum Hash gehörige Schlüssel während der Übertragung über die Luftschnittstelle ausgespäht werden kann, kann damit später dem Tag ein autorisiertes Lesegerät vorgetäuscht werden.

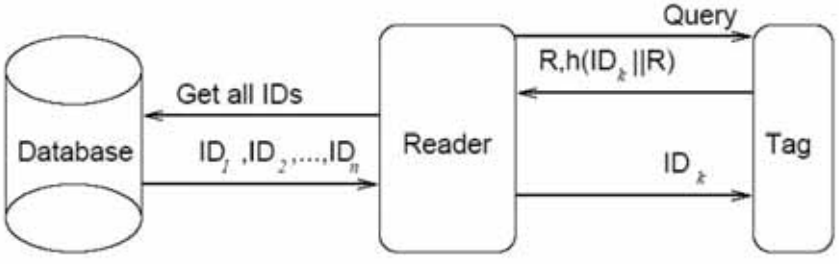

Abbildung 2: Randomized Hash-Lock-Verfahren

Randomized Hash-Lock-Verfahren

Die Sicherheit lässt sich durch das Randomized Hash-Lock-Verfahren (Abb. 2) verbessern. Hierbei sendet das Lesegerät eine Anfrage an das Tag. Anschließend generiert das Tag eine Zufallszahl, die dann an das Lesegerät gesendet wird. Lesegerät und Tag berechnen unabhängig voneinander mittels der Einwegfunktion einen Hash aus dieser Zufallszahl. Das Lesegerät sendet den resultierenden Hash an das Tag. Stimmen die beiden Hashwerte überein, wird Zugriff auf die Daten gewährt.

Dadurch, dass der Hashwert sich bei jeder Authentifizierung abhängig von der verwendeten Zufallszahl ändert, ist das Ausspähen sinnlos. Der Aufwand und die damit verbundenen Kosten für das Tag sind höher als beim einfachen Hash-Lock-Verfahren, da das Tag die Fähigkeit haben muss, Zufallszahlen zu berechnen.

Challenge-Response-Verfahren

Bei Anwendungen, die größte Sicherheit erfordern, kommen Authentifizierungsverfahren mit Verschlüsselung nach dem Challenge-Response-Prinzip (Abb. 3) zum Einsatz. Voraussetzung hierfür ist die Fähigkeit des Tags kryptographische Algorithmen zu berechnen. In der ISO-Norm 9798 werden verschiedene Challenge-Response-Verfahren für eine starke Authentifizierung bei kontaktbehafteten Chipkarten und RFID-Systemen definiert, darunter auch die gegenseitige Authentifizierung nach dem Three-pass mutual authentication protocol.

Auf ein get_challenge Kommando des Lesegeräts hin generiert das angesprochene Tag eine Zufallszahl A und sendet diese an das Lesegerät. Das Lesegerät generiert ebenfalls eine Zufallszahl B und erzeugt mit dieser und der Zufallszahl A auf Basis eines Verschlüsselungsalgorithmus und eines geheimen Schlüssels K einen verschlüsselten Datenblock (Token T) und sendet ihn an das Tag. Da beide Seiten den gleichen Verschlüsselungsalgorithmus verwenden und der Schlüssel K auf dem Tag gespeichert ist, kann das Tag den Token T entschlüsseln. Stimmen die ursprüngliche und die nun entschlüsselte Zufallszahl A und A' überein, ist die Authentizität des Lesegeräts bewiesen. Die Prozedur wird nun zur Authentifizierung des Tags gegenüber dem Lesegerät wiederholt, indem im Tag ein zweites Token S erzeugt wird.

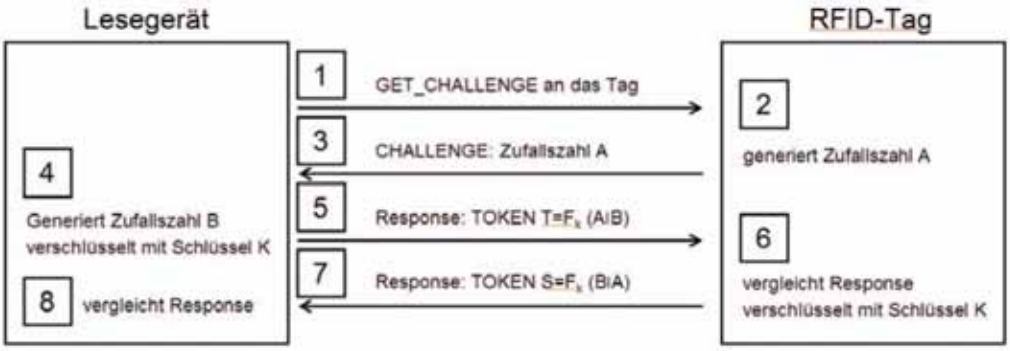

Abbildung 3: Challenge-Response-Verfahren

Bei Übereinstimmung der entschlüsselten Zufallszahlen B und B' ist auch die Authentizität des Tags gegenüber dem Lesegerät bewiesen. Da bei diesem Verfahren niemals geheime Schlüssel, sondern nur verschlüsselte Zufallszahlen über die unsichere Luftschnittstelle übertragen werden, ist ein hoher Grad an Sicherheit gegenüber unauthorisiertem Zugriff gegeben.

Auch durch Aufzeichnen und späteres Wiedervorspielen der Initialisierungssequenz (Replay-Attack) kann kein Zugriff auf das Tag oder das Lesegerät erreicht werden. Tags, die die Authentifizierung nach dem Challenge-Reponse-Prinzip ermöglichen, sind die aufwändigsten und teuersten. Neben der Berechnung von Zufallszahlen müssen sie starke Verschlüsselungsalgorithmen berechnen können. Dies ist nur mittels eines leistungsstarken Hauptprozessors oder durch die Verwendung kryptographischer Koprozessoren möglich. Dadurch wird der Preis eines einzelnen Tags in den Bereich von mehreren Euros hochgetrieben und macht damit eine Durchsetzung am Massenmarkt unmöglich. Einsatz finden solche Tags daher nicht zur Kennzeichnung von Waren, sondern beispielsweise bei Zutrittssystemen.

9.4. Datensicherheit in der Praxis

Um die Chancen von RFID zu nutzen und gleichzeitig die Bedrohung für die Persönlichkeitssphäre des Einzelnen so gering wie möglich zu halten, müssen Grundsätze eines zeitgemäßen Datenschutzrechts in RFID-Systemen bereits frühzeitig im Design-Prozess und in der Markteinführung umgesetzt werden.

Mit Hilfe von kryptographischen Verfahrenkönnen Daten verschlüsselt und somit vor dem Zugriff unberechtigter Dritter geschützt werden. Trotz kryptographischer Verfahren kann eine 100 % Sicherheit nicht garantiert werden, weil die Möglichkeit von Seitenangriffen besteht, die für jedes Anwendungsfeld individuell geprüft werden muss. Unter Seitenangriffen versteht man Angriffe, die nicht auf Schwächen der kryptographischen Verfahren basieren, sondern auf Sicherheitslücken in anderen Teilen des Gesamtsystems. Beispiele hierfür sind leicht zu erratende Passwörter, oder die Übertragung der Daten nach der Entschlüsselung über einen ungesicherten Kanal.

Weiterhin erfordern kryptographische Verfahren mit ansteigender Sicherheit und der damit verbundenen Komplexität gleichzeitig höhere technische Voraussetzungen. Dies führt zu einem Anstieg der Tag-Kosten. Im Zuge der Durchsetzung von RFID-Systemen auf dem Massenmarkt besteht gleichzeitig ein hoher Kostendruck. Er darf nicht dazu führen, dass die Datenschutzaspekte dieser Technologie außer Acht gelassen werden.

Quelle: Gabriele Spenger, Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V., http://www.fiff.de,

9.5. Der RFID-Guardian – Anti-RFID-Gerät warnt vor Datendieben

Der Wissenschaftler und bekennender RFID-Kritiker Andrew Tanenbaum von der Freien Universität Amsterdam hat im Rahmen eines Projektes mit seinen Studenten ein Anti-RFID-Gerät entwickelt. Der RFID-Guardian, wie das Gerät genannt wurde, überwacht das Umfeld des Benutzers und warnt, wenn jemand in der Nähe versucht RFID-Chips auszulesen. Die erklärte Intention des Projekts ist es, Menschen vor einer Technologie zu schützen, die zwar weltweit immer höhere Akzeptanz findet, jedoch das Potenzial besitzt, den Anspruch von Konsumenten auf Datenschutz zu kompromitieren.

»Der RFID-Guardian ist ein PDA-großes Gerät, das piepst, sobald ein aktiver RFID-Scanner in der Nähe gefunden wird«, erklärt Tanenbaum. »Die Industrie macht sich keine Gedanken darüber, ob via RFID-Tags in die Privatsphäre eingedrungen werden kann. Zudem plant die Europäische Zentralbank, Banknoten mit diesen Chips zu versehen«, kritisiert der Forscher. Somit könnten Kriminelle mit dieser Technik auf Beutesuche gehen. »Der Verbrecher geht die Straße entlang, sucht mit seinem RFID-Scanner nach prall gefüllte Geldbörsen und entscheidet sich dann für das lohnenste Ziel«, wettert Tanenbaum.

Obwohl RFID-Tags nur geringe Datenmengen speichern können, ist es Tanenbaum kürzlich gelungen einen Virus zu entwickeln, der über diese Chips eine Bedrohung für Server und Netzwerke darstellen kann. Vor allem Schadprogramme aus der Computerwelt, die einzelne Server durch eine Flut von Anfragen in die Knie zwingen, könnten auch RFID-Chips gefährlich werden, hieß es. RFID-Phishing sei ebenfalls möglich.

Die Wissenschaftler wollen das Anti-RFID-Gerät noch weiterentwickeln. Die Pläne sehen vor, dass die bislang noch auftretenden Fehler beseitigt werden und die Verbindung zwischen dem RFID-Guardian und den aufgespürten Scannern gesichert wird.

Tanenbaum ist jedoch nicht der einzige, der sich dem Schutz vor den Spychips, so die Bezeichnung der Kritiker, verschrieben hat. Das US-Unternehmen RSA Security führt einen RFID-Blocker im Programm, der das Lesegerät »verwirren« soll. Das deutsche Unternehmen Livewire hat vor wenigen Monaten eine Spezialschutzhülle entwickelt, die Datendiebstahlsicherheit für den Reisepass mit integriertem RFID-Chip bieten soll. Diese Hülle besteht aus einer in Kunststoff laminierten Aluminiumlegierung und unterbindet, dass der RFID-Chip Daten senden kann. »Die Hülle packt das Problem an der Wurzel, und verhindert, dass Unberechtigte an die gespeicherten Daten kommen können«, erklärte Livewire-Pressesprecher Stefan Horvath damals.

Unter folgedem Link finden Sie alle Details zum RFID-Guardian: http://www.rfidguardian.org/index.php/Main_Page

10. RFID IN DER KRITIK

Von interessierter Wirtschaftsseite wird es oft so dargestellt, dass Kritik an RFID grundsätzliche Technologiekritik wäre oder gar irrationale Angst vor neuer Technik. Diese Darstellung ist falsch – und am Beispiel des FoeBuD lässt sich das auch gut belegen, denn Technikfeindlichkeit kann man dieser Organisation beim besten Willen nicht nachsagen.

Die Aktiven im FoeBuD haben schon seit 1987 mit neuester Technik gearbeitet, kreativ ihre Grenzen ausgelotet und Technik auch aktiv mitgestaltet.
(Vereine wie „quintessenz", „vibe.at in Österreich oder FoeBUD „ in der BRD vergeben einmal im Jahr den an George Orwells Vision „1984" angelehnten Negativpreis „Big Brother Award")

10.1. RFID – eine Gefährdung der Privatsphäre mit neuer Qualität

Mit RFID – seinerzeit noch Transponder-Technik genannt – hatte sich der FoeBuD bereits ein paar Jahre auseinandergesetzt, bevor die Metro mit ihrem Future Store in Rheinberg bei Düsseldorf Furore machte. Und bei aller Technik-Faszination lagen für den FoeBuD die kritischen Punkte auf der Hand.

- Jede Ware, jedes einzelne Objekt erhält mit RFID eine weltweit eindeutige Seriennummer (anders als beim Strichcode, der nur die Warengruppe bezeichnet).
- RFID-Chips können berührungslos aus der Entfernung gelesen werden (auch ohne Sichtkontakt).
- Durch Registrierung und Tracking der RFID-Chips werden neue große Datensammlungen erzeugt.
- Die Seriennummer und die Information auf dem RFID-Chip sind nur scheinbar produktbezogen und anonym. Tatsächlich können sie an vielen Stellen mit persönlichen Daten der Besitzer/-innen verknüpft werden.
- Neue Datenbanken mit den RFIDChip-Seriennummern und verknüpften Informationen bieten schnellen Zugang zu großen Mengen an personenbeziehbaren Daten.
- RFID-Chips und RFID-Scanner können versteckt angebracht sein.
- Ohne dass sie es bemerken, können Bürger/-innen gescannt werden, ob sie RFID-Chips mit sich führen.
- Die Leseentfernung lässt sich unter anderem vergrößern durch Erhöhung der Sendeleistung der RFID-Scanner und durch Abschalten von Sicherheitsfeatures.
- RFID ermöglichen nicht nur Konsumprofile wie Kundenkarten schon jetzt, sondern zusätzlich detaillierte Bewegungs-, Interessen- und Kontaktprofile.

10.2. Welche Folgen hat das?

- Es entsteht die Gefahr der Überwachung.
- Tracking wird möglich durch RFID in Kleidung, Ausweispapieren, Bargeld etc.
- Gezielte Manipulation wird möglich, zB durch Nutzen der Informationen, die durch Speicherung des Bewegungs- und Interessenprofils gewonnenen werden.
- Gezielte Diskriminierung wird möglich, z.B. Preisdiskriminierung. Das heißt:

unterschiedliche Preise für unterschiedliche Menschen für dieselbe Ware im selben Supermarkt. Günstige Angebote gelten nur für profitable, wohlhabende Kunden, die außerdem per Kundenkarte bereit sind, ihre Privatsphäre preiszugeben. Das ist unsozial.

Um einige Gefahren zu verdeutlichen, muss ein wenig in die Zukunft geschaut werden - wie wir es für die Big Brother Award-Laudatio anno 2003 getan haben. (Vollständiger Text: www.bigbrotherawards.de/2003/.cop/). Einige der Zukunftsszenarien sind mittlerweile sehr bekannt und viel zitiert worden. Zum Beispiel dieses hier:

November 200?

Marion Z. bekommt einen Bußgeldbescheid der Stadt Duisburg. Das Papier eines von ihr gekauften Mars-Riegels wurde im Ententeich des Stadtparks gefunden. Marion Z. grübelt und kommt darauf, dass sie den Riegel einem Kind beim Martins-Singen geschenkt hat. Zähneknirschend zahlt sie 10 Euro Bußgeld.

Dieses Szenario hat anschaulich gemacht, was eine RFID-Kennzeichnung von Einzelprodukten bewirken kann: Jedes einzelne Produkt könnte durch die Registrierung beim Einkauf einem Menschen zugeordnet werden. Und das kann weit unangenehmere Folgen als 10 Euro Bußgeld haben. Aber auch für Arbeitnehmer/-innen könnte die Einführung von RFID zu unangenehmen Überraschungen führen:

Juni 200?

Als Supermarkt-Fachkraft Gerd J. abends nach Hause kommt, liegt dort ein Brief seiner Geschäftsleitung mit einer Abmahnung. Er sei in den vergangenen Wochen durchschnittlich 9 Mal auf der Toilette gewesen und habe dort pro Tag ca. 72 Minuten zugebracht. Das liege 27 Minuten über dem Soll und diese Zeit werde ihm zukünftig von seinem Arbeitszeitkonto abgezogen. Entsetzt sucht er seinen Supermarkt-Kittel ab und findet einen RFID im Kragensaum.

Arbeitskleidung mit integrierten RFIDChips und Seifenspender, die anhand des Chips kontrollieren, ob sich jemand die Hände gewaschen hat, sind in den USA bereits Realität.

10.3. Forderungen zu RFID

- Wichtigster Grundsatz: Datenvermeidung und Datensparsamkeit. Daten, die nicht notwendig sind, dürfen gar nicht erst erfasst werden. Und: Es sollen so wenig wie möglich persönliche Daten erhoben, gespeichert und verarbeitet werden.

- Transparenz. Das heißt: Sowohl RFIDChips als auch RFID-Scanner müssen, wo immer sie sind, deutlich sichtbar mit einem Warnhinweis gekennzeichnet werden.

- Datenschutz muss Standard sein. Das bedeutet, Opt-Out-Lösungen, wo die Kundinnen erst tätig werden müssen, um ihre Privatsphäre zu schützen, sind nicht akzeptabel. So zum Beispiel der sogenannte Deaktivator im Future Store – der ist definitiv keine Lösung.Bislang müssen sich Kundinnen und Kunden noch einmal neu anstellen, nachdem sie die Kasse passiert haben, und jedes einzelne Produkt auf den Deaktivator stellen, um den auf dem RFID-Chip gespeicherten Nummerncode mit Nullen zu überschreiben. Solche Opt-Out-Lösungen haben lediglich Alibifunktion. Außerdem bleibt bei diesem Verfahren die weltweit einmalige Seriennummer jedes Artikels erhalten und kann weiter verarbeitet werden.

- Das Tracking von Personen ist völlig abzulehnen, sowohl direkt als auch indirekt. Die RFID-Industrie argumentiert oft, dass die Nummern auf den RFID-Chips „nicht personenbezogen" seien, sondern nur Informationen zum Produkt enthalten würden. Dies stimmt aber nur auf den ersten Blick. Sobald nämlich auch nur an einer einzigen Stelle – zB durch das Zahlen mit Kredit- oder EC-Karte oder das Registrieren-Lassen einer Kundenkarte die Verbindung von einem dieser RFID-Chips zu einer Person hergestellt werden kann, können auch die Informationen aller anderen RFID-Chips, die diese Person trägt, mit ihren persönlichen Daten verknüpft werden. Mit anderen Worten: Die Daten auf den RFID-Chips sind personenbeziehbar. Wenn RFID-Chips auf Einzelprodukt- Ebene eingeführt würden, trügen Bürgerinnen und Bürger aus der Ferne identifizierbare Dinge bei sich und könnten niemals sicher sein, ob nicht doch eine Verknüpfung dieser Produktdaten mit ihren persönlichen Daten geschieht und damit z.B. Bewegungs- und Interessenprofile von ihnen erstellt werden können.

- Keine RFID-Chips auf Einzelprodukten (item level)

- Keine RFID-Chips auf Produkten in auch von Kund-innen genutzten Räumen, also zum Beispiel in den Verkaufsräumen. Wenn RFID-Technik in der Logistik bis hin zu den Lagerräumen zum Einsatz kommt, ist das zunächst kein Problem für die Verbraucherinnen und Verbraucher (möglicherweise aber für die Arbeitnehmer/- innen!).

- Keine RFID-Chips in Bargeld. Es muss auch in Zukunft möglich sein etwas zu bezahlen, ohne eine Datenspur zu hinterlassen.

- Keine RFID-Chips in Reisepässen, Personalausweisen oder sonstigen Ausweisdokumenten. Wenn Bürger nicht sicher sein können, ob sie ohne ihr Wissen jederzeit und überall identifiziert werden können, werden sie in Zukunft möglicherweise zögern, ihr Recht auf freie Meinungsäußerung oder Versammlungsfreiheit wahrzunehmen.

10.4. Fazit

Wir brauchen datenschutzfreundliche Technik (Privacy Enhancing Technologies). Wenn eine technische Infrastruktur erst einmal in einer bestimmten Form allgemein installiert ist, kann sie kaum noch geändert werden. Wenn die Technik nicht von vornherein so gestaltet ist, dass sie Missbrauch schwer oder unmöglich macht, wird er früher oder später passieren – legal oder illegal. Mit der RFID-Technik kann auch etwas anderes passieren: Wenn die Verbraucher/-innen die möglichen negativen Konsequenzen der Technik erst einmal kennen und merken, dass ihre Interessen ignoriert und ihre Besorgnis nicht ernstgenommen wird, dann werden sie die RFIDTechnik nicht annehmen, sondern boykottieren. Späteres Nachbessern an der Technik wird teuer und kann den Schaden kaum wieder gutmachen.

Wir brauchen Gesetze, die den neuen Gefährdungen wirksam begegnen Die RFID-Industrie und ihre Lobbyverbände bemühen sich intensiv, eine gesetzliche Regulierung von RFID abzuwehren, indem sie sogenannte Selbstverpflichtungserklärungen propagieren. Diese sollten jedoch zutreffender unverbindliche Absichtserklärungen genannt werden. Es leuchtet nicht ein, warum Firmen, die stets beteuern, nichts Böses mit den gewonnenen Daten machen zu wollen, Angst vor einer gesetzlichen Regulierung haben. Denn eine gesetzliche Regulierung würde die good guys schützen, also die Firmen, die die Privatsphäre der Bürger tatsächlich achten, – und zwar sowohl vor der böswilligen Konkurrenz als auch vor ihren eigenen Aktionären. Wenn einige Firmen meinen, sie könnten die RFID-Einführung wie geplant durchziehen und müssten nun – angesichts der wachsenden Abneigung der Öffentlichkeit gegen eine Allgegenwart von Schnüffelchips – lediglich etwas mehr in Lobbyarbeit, Marketing und Public Relations investieren, um kritische Stimmen platt zu machen – dann unterliegen sie einem gefährlichen Irrtum. Wir haben zur Zeit die einmalige Chance, bei der RFID-Technologie die Richtung mit zu bestimmen. Wir müssen uns entscheiden, ob wir für eine Kontrollgesellschaft oder für eine lebenswerte Welt arbeiten.

Quelle: Rena Tangens, Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V., http://www.fiff.de, http://www.foebud.org, http://www.bigbrotherawards.de, http://www.stoprfid.de

Quellen:

http://www.bsi.de

http://www.btq-kassel.de

http://www.computerpartner.de

http://www.foebud.org

http://www.heise.de

http://www.netzwelt.de

http://www.nocards.org/(englisch)

http://www.rfid-informationen.de

http://www.rfidvirus.org

http://www.telepolis.de

http://www.datenschutzverein.de/presse.html

http://www.die-gesundheitskarte.de/testphase/testregionen/index.html

http://www.ecin.de/news/2005/04/11/08177

http://www.electronicstalk.com/news/jui/jui100.html

http/www.elektrosmog.com

http://www.environmental-studies.de/Info/RFID/RF-11/rf-11.html

http/www.foebud.org

Notizen

Jetzt Mitglied werden!

Familienname ..... Vorname ..... ❒ Frau ❒ Herr

SV-Nr./Geburtsdatum | | | | | | | | | | Akad. Grad .....Geburtsname .....

Straße/Haus-Nr. ..... PLZ/Wohnort .....

Telefonisch erreichbar ..... **E-Mail** .....

❒ Angestellte/r ❒ Lehrling ❒ Werkvertrag ❒ geringfügig beschäftigt ❒ Freier Dienstvertrag ❒ Selbstständig (Gewerbeschein)
❒ Zeitarbeitskraft ❒ SchülerIn ❒ StudentIn ❒ dzt. ohne Beschäftigung ❒ Zweitmitgliedschaft ❒ FacharbeiterIn

Derzeitige Tätigkeit ..... ❒ Ich war bereits Mitglied der Gewerkschaft von/bis .....

Ihre Angaben werden **streng vertraulich** behandelt und unterliegen dem **Datenschutz**. Nach Zusendung Ihrer Anmeldebestätigung haben Sie unter Verwendung Ihrer Mitgliedsnummer die Möglichkeit, sämtliche für Sie wichtigen Informationen wie Kollektivvertrag, Informationen zu aktuellen Themen, Aktivitäten unserer Interessengemeinschaft, etc., einzuholen. Unsere Internetadresse: **www.gpa-djp.at**

Beschäftigt bei Firma (bzw. Schule/Universität) ..... Dienstort.....

Anschrift .....

Branche ..... WerberIn-Mitgliedsnummer.....

Die Betragszahlung erfolgt mit Einzugsermächtigungsverfahren.

Hiermit ermächtige ich Sie **widerruflich**, die von mir zu entrichtenden Zahlungen bei Fälligkeit zu Lasten meines Kontos mittels Lastschrift einzuziehen. Damit ist auch meine kontoführende Bank ermächtigt, die Lastschriften einzulösen, wobei für diese keine Verpflichtung zur Einlösung besteht, insbesondere dann, wenn mein Konto die erforderliche Deckung nicht aufweist. Ich habe das Recht, innerhalb von 42 Kalendertagen ab Abbuchungstag ohne Angabe von Gründen die Rückbuchung bei meiner Bank zu veranlassen. Ich ermächtige die Gewerkschaft der Privatangestellten, Druck, Journalismus, Papier (GPA-djp) den folgenden Mitgliedsbeitrag (= 1 % meines Bruttogehaltes/Bruttolohnes, meiner Bruttolehrlingsentschädigung bzw. Grenzbeitrag) von meinem unten angeführten Konto einzuziehen:

Höhe des monatlichen Beitrages: **EUR** | | | | |

❒ monatlich ❒ alle 2 Monate ❒ jedes Quartal ❒ 1/2 jährlich ❒ jährlich (Schüler-/StudentInnen, Zweitmitgliedschaft)

Konto-Nr. | | | | | | | | | | Geldinstitut ..... Bankleitzahl | | | | |

Im Jänner jeden Kalenderjahres erhalte ich gemeinsam mit der Finanzamtsbestätigung eine Information für die Anpassung meines Beitrages. Basis für den Prozentsatz der Anhebung ist ein gewichteter Durchschnitt von bestimmten Kollektivvertragsabschlüssen der GPA-djp innerhalb eines Beobachtungszeitraumes von 12 Monaten. Sollte ich mit der Anpassung nicht einverstanden sein, habe ich die Möglichkeit, mit dem beigelegten Formular den tatsächlich gültigen Mitgliedsbeitrag bekannt zu geben.

Nur ankreuzen wenn ein Betriebsabzug gewünscht wird:

❒ Betriebsabzug - da in meinem Betrieb ein Betriebsabzug möglich ist, erkläre ich mich einverstanden, dass mein Gewerkschaftsbeitrag durch den Arbeitgeber (Dienstgeber) von meinem Gehalt/Lohn, meiner Lehrlingsentschädigung abgezogen wird. Ich ermächtige den Arbeitgeber, alle im Zusammenhang mit der Betragseinhebung erforderlichen personenbezogenen Daten im Sinne des DSG § 18 (1) bzw. § 7 (1) an die GPA-djp zu übermitteln. Sollte ich den Gehalts/Lohnabzug, Lehrlingsentschädigungsabzug im Betrieb nicht mehr wünschen oder ich aus dem Betrieb ausscheiden, kann die Zahlungsart ohne Rücksprache auf Einzugsermächtigungsverfahren umgestellt werden. Ich habe das Recht, innerhalb von 42 Kalendertagen ab Abbuchungstag ohne Angabe von Gründen die Rückbuchung bei meiner Bank zu veranlassen.

| | | | | | |

Beitrittsmonat/-jahr

.....

Datum/Unterschrift (Diese Unterschrift gilt gleichzeitig als Berechtigung für o.a. Einzugsermächtigungsverfahren.)

GPA djp
GEWERKSCHAFT DER PRIVATANGESTELLTEN
DRUCK – JOURNALISMUS – PAPIER

1034 Wien, Alfred-Dallinger-Platz 1, Telefon 05 0301-301, Fax 05 0301-300, eMail: service@gpa-djp.at

DVR 0046655, ZVR 576 439 352

mitmachen - mitreden - mitbestimmen

Interessengemeinschaften

Ihr Zusatznutzen ohne Extrakosten

Interessengemeinschaften (IGs) der GPA-djp bringen Menschen mit ähnlichen Berufsmerkmalen zusammen. Zum Austauschen von Erfahrungen und Wissen, zum Diskutieren von Problemen, zum Suchen kompetenter Lösungen, zum Durchsetzen gemeinsamer beruflicher Interessen. **Mit Ihrer persönlichen Eintragung in eine oder mehrere berufliche Interessengemeinschaften**

>> erhalten Sie mittels Newsletter (elektronisch oder brieflich) regelmäßig Informationen über Anliegen, Aktivitäten und Einladungen für Ihre Berufsgruppe;

>> können Sie Ihre beruflichen Interessen auf direktem Weg in die Kollektivvertragsverhandlungen Ihres Branchenbereichs einbringen;

>> erschließen Sie sich Mitwirkungsmöglichkeiten an Projekten, Bildungsveranstaltungen, Kampagnen, Internet-Foren und anderen für Ihre Berufsgruppe maßgeschneiderten Veranstaltungen, auch auf regionaler Ebene;

>> nehmen Sie von der Interessengemeinschaft entwickelte berufsspezifische Dienstleistungen und Produkte in Anspruch (Fachberatung auf regionaler Ebene, Bücher, Broschüren und andere Materialien);

>> beteiligen Sie sich an demokratischen Direktwahlen Ihrer beruflichen Vertretung auf bundes- und regionaler Ebene und nehmen dadurch Einfluss auf die gewerkschaftliche Meinungsbildung und Entscheidung.

www.gpa-djp.at/interesse

work@professional für GeschäftsführerInnen, TeamleiterInnen, KonstrukteurInnen, DirektorInnen, TechnikerInnen, WissenschaftlerInnen, MeisterInnen, freiberufliche ManagerInnen, Abteilungs-, ProjektleiterInnen, ÄrztInnen, SpezialistInnen auf anderen Gebieten - kurz FachexpertInnen und Führungskräfte.

work@flex für WerkvertragnehmerInnen, freie DienstvertragnehmerInnen und GewerbescheininhaberInnen ohne eigene Angestellten.

work@social für Alten-, Kranken-, BehindertenbetreuerInnen, SozialarbeiterInnen, aber auch Angestellte in sozialen Berufen.

work@IT für IT-SpezialistInnen, MitarbeiterInnen bei EDV-Projekten, im Internet und neuen Medien sowie in der Telekommunikation.

work@education für ErwachsenenbildnerInnen, (freie) TrainerInnen, LehrerInnen an Fachhochschulen und Privatuniversitäten, Menschen in Beratungsberufen.

work@external für AußendienstmitarbeiterInnen, ServicetechnikerInnen, mobile KrankenpflegerInnen, BaustellenleiterInnen, LeiterInnen internationaler Forschungsprojekte, ForstaufseherInnen oder KundenbetreuerInnen von Versicherungen.

work@migration für Menschen die in Österreich ohne österreichische Staatsbürgerschaft leben bzw. diese erst während Ihres Aufenthaltes erwerben, MitarbeiterInnen in Beratungsstellen, in Initiativen von MigrantInnen, ÖsterreicherInnen, die in einem fremden Land leben sowie Menschen, denen dieses Thema wichtig ist.

Ich möchte mich in folgende Interessengemeinschaften eintragen.

❑ work@professional ❑ work@flex ❑ work@social ❑ work@external ❑ work@education ❑ work@IT ❑ work@migation

Dieses Service ist für mich kostenlos.

❑ Frau ❑ Herr Akad. Grad .....

Familienname ..... Vorname .....

Berufsbezeichnung. ..... Betrieb.....

Telefonisch erreichbar ..... **E-Mail** .....

GPA djp
GEWERKSCHAFT DER PRIVATANGESTELLTEN
DRUCK – JOURNALISMUS – PAPIER

.....
Datum/Unterschrift

1034 Wien, Alfred-Dallinger-Platz 1, Telefon 05 0301-301, Fax 05 0301-300, eMail: service@gpa-djp.at

DVR 0046655, ZVR 576 439 352

GPA-DJP Kontaktadressen

Service-Hotline: 05 0301-301

GPA-djp Service-Center

1034 Wien, Alfred-Dallinger-Platz 1
eMail: service@gpa-djp.at
Fax: 05 0301-300

Regionalgeschäftsstelle Wien
1034 Wien, Alfred-Dallinger-Platz 1

Regionalgeschäftsstelle Niederösterreich
3100 St. Pölten, Gewerkschaftsplatz 1

Regionalgeschäftsstelle Burgenland
7000 Eisenstadt, Wiener Straße 7

Regionalgeschäftsstelle Steiermark
8020 Graz, Karl-Morre-Straße 32

Regionalgeschäftsstelle Kärnten
9020 Klagenfurt, Bahnhofstr. 44/4

Regionalgeschäftsstelle Oberösterreich
4020 Linz, Volksgartenstraße 40

Regionalgeschäftsstelle Salzburg
5020 Salzburg, Markus-Sittikus-Str. 10

Regionalgeschäftsstelle Tirol
6020 Innsbruck, Südtiroler Platz 14

Regionalgeschäftsstelle Vorarlberg
6900 Bregenz, Reutegasse 11

www.gpa-djp.at

Es gibt vieles,

für das es sich lohnt,
organisiert zu sein.

service@gpa-djp.at

ver.di-innotec

GPA djp
GEWERKSCHAFT DER PRIVATANGESTELLTEN
DRUCK – JOURNALISMUS – PAPIER

FIfF

1034 Wien, Alfred-Dallinger-Platz 1, Telefon: 05 0301-301, Fax: 05 0301-300 - **eMail: service@gpa-djp.at**